
Wells Fargo International Non-Employee and Contingent Resource Privacy Notice

This Notice applies to all countries except for the following: the United States, Brazil, European Union countries, the United Kingdom, and the Dubai International Financial Center.

Effective: 17 April 2025

The relevant Wells Fargo entity ("**we**", "**us**", "**our**" or the "**Company**") which has engaged the vendor or third-party organization that employs or engages you (collectively, "**Vendor**") provides this Privacy Notice ("**Notice**") to explain how the Company will Process your Personal Data during and after your organization's engagement with Wells Fargo, Wells Fargo's privacy practices, and your rights over your Personal Data. Under the Vendor engagement, you will be providing or facilitating the provision of certain services to us on behalf of the Vendor. As part of the Vendor engagement, information directly or indirectly identifying you or individuals relating to you ("**Personal Data**") may be collected by us and/or provided to us by the Vendor. The Company will act as the data controller regarding the collection, use, storage, transfer, handling and any other processing activity (collectively, "**processing**" or "**process**") relating to your Personal Data. If you are engaged by Wells Fargo in one of the excluded countries listed above, a different privacy notice will govern the engaging entity's Personal Data processing activities.

1. What Personal Data Do We Collect?

We may collect the following categories of Personal Data in connection with the Vendor engagement:

- **Master data:** such as name (first name, last name, family name), date of birth, and government-issued identification documents (to the extent permitted by law) and photograph.
- **Work contact details:** such as name, work address, work phone numbers, fax numbers, and work email address.
- **Visa and work permit data:** existing and expired visa(s) and other work permit details relating to you and/or individuals related to you (e.g., spouse, family members).
- **Emergency contact information:** such as name and contact information (if provided by you) of a family member or your nominated person to be contacted in an emergency.
- **Absence data:** such as dates of absence and reasons for absence (such as medical leave) to the extent these apply to you.
- **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 engagement by Wells Fargo; (ii) is a U.S. or non-U.S. government official; or (iii) has decision making authority or capability over any matters affecting Wells Fargo; and any other Personal Data relating to another individual which you may provide directly or indirectly to the Company.
- **Performance data:** such as information pertaining to the quality and efficiency of the services you are rendering on behalf of the Vendor, against the agreed benchmarks between the Company and the Vendor and other similar assessment of performance.

- **Organizational data:** such as title, job position, function, worker 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.
- **Engagement data:** such as data that may be collected during your engagement including from use of Wells Fargo facilities, company transportation or as part of training activities and participation in Wells Fargo surveys, initiatives attendance photographs and videos at Company or events.
- **Usage and monitoring data:** such as data about when and how you use and interact with equipment, systems, communication channels, software (including those you install), and property, such as computers, mobile devices, email, internet, calendar invitations, shared files, instant message or chat, video and/or audio calls, recordings and transcriptions, internet, geolocation, 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 Wells Fargo business premises; information about your location; office access data; device data relating to personal electronic devices or other equipment used for any Bring Your Own Device (“**BYOD**”) program (if applicable to you), e.g. device name, OS or model.
- **Disciplinary data:** such as information pertaining conduct, internal Wells Fargo investigations, and disciplinary and grievance matters.
- **Health-related data:** health-related data relevant to promoting and ensuring public or workplace health and safety (e.g., in connection with the COVID-19 pandemic), such as body temperature, symptoms, recent travel, potential or confirmed exposure, testing (including results) and vaccination status.
- **Personal Data contained in communications:** such as the types of Personal Data listed above that may be contained in emails, phone calls, video calls, instant messages, chats or other communications made or received on any corporate or Wells Fargo-approved device, on any BYOD-related personal device, or through any other means of Wells Fargo related communications, which may be reviewed as part of risk management, compliance, and other service engagement or business activities.
- **Criminal records data:** criminal records properly obtained through a lawful background reference check may be collected for legal, compliance, risk management and other purposes.
- **Biometric data:** biometric data such as fingerprints, keystrokes, hand scans, biometric algorithms, or voice prints may be collected if you are required to access or use systems with biometric safeguards or features.
- **Financial information:** 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), may be collected legal, compliance, risk management and other purposes.

Amongst the types of Personal Data listed above, some of them may be considered sensitive under the data protection laws where you are engaged. What Personal Data is considered sensitive depends on the data protection law where you are engaged. Examples of sensitive Personal Data may include specific identity information (e.g., governmental identity documents); personal whereabouts (including geolocation data); health-related data (such as medical reports); financial data (such as your investment accounts or transactions); criminal records; biometric data (such as fingerprints, voice prints, and other physical, physiological or behavioral characteristics); political affiliation; trade union membership; 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, or any other third party individuals (for example, for emergency contact 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.

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. It is necessary that you provide the Company with your Personal Data (including sensitive Personal Data), without which we will not be able to administer our engagement with the Vendor where it requires the processing of your Personal Data.

2. Why We Process Your Personal Data?

The Company may process the types of Personal Data listed in [Section 1](#) to enable you to provide services to us under our engagement with the Vendor, including processing the following categories of Personal Data for the following purposes (“**Engagement Purposes**”).

- a) **Human resource management purposes relating to handling, maintaining, and improving administration of our engagement with the Vendor and related business operations.** For example: assigning projects and tasks; conducting resource analysis and planning; administering project costing and estimates; managing work activities and administering compliance trainings; providing physical access to Wells Fargo offices/locations and issuing access passes or other credentials; Vendor evaluation, engagement and relationship management; providing performance metrics to the Vendor (as your employer or agency) including assessment of the quality and quantity of the services provided under our agreement with the Vendor; determining and managing your suitability to be engaged to provide services to Wells Fargo on behalf of the Vendor (e.g., in instances including where the Vendor engagement requires providing you access to Wells Fargo's network, to determine whether you appear on internal “Do Not Hire” or “Do Not Reengage” lists, to place and maintain your Personal Data on such lists for future consideration, to determine at Wells Fargo's discretion if you have committed a crime or violation of internal policies and codes of conduct). For this purpose, the Company may process master data, work contact details, visa and work permit data, performance data, absence data, engagement data, disciplinary data, and other categories of Personal Data where needed.
- b) **Human resource management purposes relating to maintaining a corporate directory and offer platforms for sharing information,** including populating such directories and platforms, making contact details available, and making intranet websites accessible by staff and contingent works, to facilitate staff communication and sharing of information internally providing company transportation. For this purpose, the Company may process Personal Data such as master data, work contact details, organizational data, engagement data, data you voluntarily submit for these purposes, and other categories of Personal Data where needed.
- c) **Human resource management purposes in the event of emergencies,** such as contacting you, your family or emergency contacts, protecting the health and safety of staff 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.
- d) **Technology management purposes.** For example: implementing, maintaining and upgrading information, cloud and other technology systems, applications 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 your 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, organizational data, engagement data, usage and monitoring data, Personal Data contained in communications, disciplinary data, and other categories of Personal Data where needed.

- e) **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, regulatory 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, staff, confidential or restricted data; protecting Company, customer and third party data and assets; managing and mitigating risk; avoiding actual or perceived conflicts of interest; meeting regulatory expectations; conducting internal audits and investigations; ensuring compliance with internal Human Resources 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 master data, work contact details, organizational data, absence data, performance data, engagement data, third party data, usage and monitoring data, disciplinary data, Personal Data contained in communications, and other categories of Personal Data where needed.
- f) **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 claims or proceedings involving any Wells Fargo entity.** For example: complying with requests from regulators or other authorities in your home country or other jurisdictions; participating in legal proceedings including domestic and cross-border litigation and discovery procedures; and complying with requests from police and/or other law enforcement authorities. For this purpose, the Company may process Personal Data such as master data, work contact details, organizational data, engagement data, absence data, emergency contact information, performance data, usage and monitoring data, disciplinary data, third party data, Personal Data contained in communications, and any other category of Personal Data necessary to respond to the request, demand, claim or proceedings.
- g) **Legal, risk and compliance purposes relating to complying with worker or workplace-related legal requirements.** For example: complying with requirements pertaining to income tax, national insurance deductions, and applicable laws relating to workers and immigration. For this purpose, the Company may process master data, work contact details, engagement data, organizational data, absence data, and other categories of Personal Data where needed.
- h) **Corporate restructuring purposes relating to conducting Merger & Acquisition (M&A) transactions, restructuring, business transfers, combinations, and similar or related activities.** For this purpose, the Company may process any category of Personal Data necessary to achieve the purpose.
- i) **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 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 cease providing services to the Company. Please see [Section 5](#) below for further information about how long we retain Personal Data.

3. Transfers of Personal Data to Other Recipients

Wells Fargo operates across the globe, and we may transfer Personal Data to recipients located in other countries to facilitate this. In particular, the Company may transfer the types of Personal Data described in [Section 1](#) to the following recipients to be processed for the Engagement 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 Engagement Purposes. A non-exhaustive list 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.** As necessary in connection with the Engagement Purposes, Personal Data may be transferred by the Wells Fargo Group to customers, prospects and other third parties.
- **Regulators and authorities.** As necessary for the Engagement Purposes described above, Personal Data may be transferred by the Wells Fargo Group to regulators, courts, and other authorities (e.g., tax and law enforcement authorities).
- **Service providers.** As necessary for the Engagement Purposes described above, Personal Data may be shared with one or more parties providing services to the Wells Fargo Group, whether affiliated or unaffiliated, to process Personal Data under appropriate instructions ("**Data Processors**"). Such Data Processors (also known as entrusted persons under some applicable laws) 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. Data Processors may carry out instructions related to IT system support, cloud computing or services, training, compliance, supporting the Engagement Purposes, or other legitimate activities, 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 a Data Processor but also as a data controller, such service providers will be subject to any necessary contractual obligations or other safeguards regarding the protection and processing of Personal Data.
- **Entities relating to business transfers, combinations and similar 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, to the extent permitted by law, be transferred by the Wells Fargo Group to entities related to these transactions to facilitate the service engagement with the Vendor (i.e., your employer or agency) or for other Engagement Purposes.

Access to Personal Data within the Company will be limited to those who need to know the information for the Engagement Purposes list in [Section 2](#) and will include but may not be limited to your managers and their designees, and personnel in HR, IT, Compliance, Legal, Finance and Accounting, and in Internal Audit. All personnel within Wells Fargo will generally have access to non-sensitive business contact information such as your name, position, telephone number, work address, and email address.

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 Engagement Purposes described above. Other country-specific information about transfers of personal data may be found in [Section 9](#).

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 Personal Data in accordance with Wells Fargo's standards. 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 8](#).

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 a contingent resource with us).
- Whether there is a legal obligation to which we are subject (for example, certain laws may require us to keep records of your engagement for a certain period of time after you are no longer engaged as a contingent resource with us).
- Whether retention is advisable considering 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).

Please bear in mind that if, as a result of your engagement, you have access to Personal Data of the Company or any of its controlling, subsidiary or affiliated entities, its clients and/or service providers or any third parties, you are obliged to maintain the confidentiality of such Personal Data and are prohibited from sharing such Personal Data with third parties, without authorization of the Company or the individuals. This obligation subsists even after the termination of your engagement.

6. 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; corporate usage, activities or communications pertaining to devices relating to any BYOD program; and CCTV recordings, etc. The Company may engage in such activities to administer IT access, provide IT support, manage security services, and staff authorizations, manage risk, 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 Human Resources and Return to Office policies), and to fulfil other Engagement 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 Wells Fargo's 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 legal, compliance, risk management and other Engagement 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 Engagement 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 you 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 engaged, you may have the following rights over your Personal Data:

- Right to confirm whether your Personal Data is being processed.
- 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, rectify, update or complete your Personal Data.
- Right to suspend, restrict or object to processing of your Personal Data.
- Right to delete or erase your Personal Data.
- Right to portability of your Personal Data.
- Right to consent, elect the scope of consent, or withdraw consent, to the processing of your Personal Data. Withdrawal of consent will not affect the lawfulness of processing done prior to withdrawal, or processing conducted on legal bases 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 engaged.
- Right to refuse and request for explanations regarding automated decision-making using your Personal Data (if any).
- If you are engaged by Wells Fargo in the People's Republic of China ("**China**")¹, rights in relation to the following:
 - Where required by data privacy laws in China, the Company will enter 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.
 - If you are engaged by Wells Fargo in 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 applicable

¹ 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.

law. Requests or questions concerning these Standard Contract(s) may be directed to us using the contact details in [Section 8](#).

- If you are engaged by Wells Fargo in Japan, rights to:
 - obtain information about transfer safeguards implemented with respect to overseas transfers of your Personal Data by the Company;
 - be provided with information about security measures implemented to protect your Personal Data; and
 - be informed of the name of the Data Privacy Officer.
- If you are engaged by Wells Fargo in India, you may have the following rights upon the Digital Data Protection Act 2023 (or the relevant provisions of the Act granting these rights) coming into force:
 - request for a summary of personal data processed and the processing activities undertaken by the Company;
 - request for the identities of data recipients with whom personal data has been shared and a description of the personal data shared with such recipients;
 - have your grievances redressed;
 - nominate any other individual who, in the event of your death or incapacity, can exercise your data subject rights; and
 - request for the contents of this Notice to be provided in any language specified in the Eight Schedule to the Constitution of India.

The abovementioned rights are not absolute and may be subject to exceptions or limitations depending on the applicable data protection law where you are engaged. 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. In addition to the Data Privacy Officers, the Company has appointed a 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. 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

The Company has appointed the Regional Privacy Officers (as listed below) who are responsible for responding to requests in relation to your Personal Data.

| Region | Contact Details |
|--------------------------|---|
| Asia-Pacific | APAC Regional Data Privacy Officer 138 Market Street, #30-01, CapitaGreen Singapore, 048946 Telephone: (65) 6395 6900 Email: privacy.apac@wellsfargo.com |
| Canada and Latin America | Americas Regional Privacy Officer 23 rd Floor, 22 Adelaide Street West |

| | |
|-------------|--|
| | <p>Toronto, Ontario Canada M5H-4E3 Telephone: (416) 607-2900 Email for Canada: canadaprivacyinfo@wellsfargo.com Email for Latin America: privacy.latinamerica@wellsfargo.com</p> |
| India | <p>India Grievance Officers Wells Fargo Bank N.A. Mumbai Representative Office Peter Tan peter.tan@wellsfargo.com</p> <p>Wells Fargo International Solutions Private Limited Vijayalakshmi Kannan IP.Privacy@wellsfargo.com</p> |
| South Korea | <p>South Korea Data Privacy Officer</p> <p>Youngmi Kim Wells Fargo Bank, N.A. Seoul Branch 21/F, D1, D Tower, 17 Jong-ro 3-gil, Jongno-gu, Seoul, 03155, Korea Telephone: (82) 2-3706-3187 Email: Youngmi.Kim@wellsfargo.com</p> |
| Philippines | <p>Philippines Data Protection Officer</p> <p>Wells Fargo International Solutions LLC – Philippines 1180 Wells Fargo Drive, McKinley Hill, Dr. Taguig, Philippines IP.Privacy@wellsfargo.com</p> <p>Wells Fargo International Clearing Support Services, LLC – Philippine Branch 17th Floor, Five Neo Building, E-Square IT Park 31st St., Zamora Circle Bonifacio Global City, Fort Bonifacio, Taguig City WFICSS.privacy@wellsfargo.com</p> <p>Contact information for the Data Protection Authority in the Philippines is available at: https://www.privacy.gov.ph/.</p> |

9. Other Country-Specific Information

If you are engaged by Wells Fargo in any of the listed countries below, please see additional country-specific privacy information for the relevant country below.

Australia

Our Wells Fargo entities in Australia covered by this Notice are as follows:

| Entity Name | Address |
|-------------|---------|
|-------------|---------|

| | |
|---|---|
| Wells Fargo Bank, N.A. - Sydney, Australia | Level 8, 88 Phillip Street, Aurora Place, Sydney, NSW 2000 |
| Wells Fargo International Finance (Australia) Pty Ltd | Private Office 10.07, Level 7, 80 Collins Street, Melbourne, VIC 3000 |

China

Our Wells Fargo entities in China covered by this Notice are as follows:

| 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 |

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:

| Name of the Data Controller in China | Contact Details | Personal Data Transferred | Processing Purpose | Processing Means | Retention Period | Method and Procedure to Exercise Rights |
|--|--|--|--|--|---|--|
| The Company's Affiliated Entities (defined in Section 3) in China such as those listed in the table immediately above | They may be contacted through the APAC Regional Privacy Officer using the contact details in Section 8 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 8 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 | Personal Data Transferred | Processing Purpose | Processing Means | Retention Period | Method and Procedure to Exercise Rights |
|---|--|--|--|--|---|---|
| The Company's Affiliated Entities (defined in Section 3) such as Wells | Offshore recipients can be contacted through the APAC Regional Privacy Officer using the contact | 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 |

Fargo & details in [Section 8](#) above
Company, etc.

in [Section 8](#)
above

Wells Fargo takes appropriate technical, physical, and organizational security measures to protect Personal Data collected or originating from China.

- 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 Wells Fargo'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 Wells Fargo's networks for actual or potential attacks or breaches. Wells Fargo'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, 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.
- 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.

Japan

Our Wells Fargo entities in Japan covered by this Notice are as follows:

| Entity Name and Representative | Address |
|---|--|
| 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 |
| 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 |

To the extent that the sharing of Personal Data with the recipients listed in [Section 3](#) is subject to any Japanese data protection laws, where applicable, the Wells Fargo Japan entity above which you are engaged by may jointly use Personal Data with those recipients such as its Affiliated Entities. That entity is responsible for the management of Personal Data shared with such recipients, and the name of the Company's representative is listed above. 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 for additional information about these safeguards.



New Zealand

Our Wells Fargo entity in New Zealand covered by this Notice is as follows:

| Entity Name | Address |
|---|---|
| Wells Fargo International Finance (New Zealand) Limited | North Lobby, Level 1, Office #108, 293 Durham Street, Christchurch, 8013, New Zealand |

Philippines

In compliance with the Philippines Data Privacy Act of 2012, its implementing rules and regulations, and other relevant issuances, Wells Fargo International Solutions LLC – Philippines (WFIS) and Wells Fargo International Clearing Support Services, LLC – Philippine Branch (WFICSS) were registered with the NPC, along with its Data Processing Systems and appointed Data Protection Officer. These entities have been issued seals of registration by the NPC, which are displayed below.

| Wells Fargo International Solutions LLC – Philippines | Wells Fargo International Clearing Support Services, LLC – Philippine Branch |
|--|--|
|  |  |

South Korea

Your Personal Data may be transferred electronically (e.g., by IT network, etc.) or physically (e.g., by courier, post, etc.), including outside South Korea, to the third party recipients listed in [Section 3](#) during your engagement with the Company and/or within the periods of retention and use explained in [Section 5](#). You may contact us using the details in [Section 8](#) for queries relating to offshore recipients of your Personal Data.

Taiwan

Our Wells Fargo entity in Taiwan covered by this Notice is as follows:

| Entity Name | Address |
|--|--|
| Wells Fargo Bank, N.A. – Taipei Branch | No.44, 17F, Chung Shan North Road, Section 2 Taipei City, Taiwan |

Vietnam

Our Wells Fargo entity in Vietnam covered by this Notice is as follows:

| Entity Name | Address |
|---|---|
| Wells Fargo Bank N.A. Hanoi Representative Office | No. 16, Phan Chu Trinh Street, Unit 1410, Cornerstone Building, Hoan Kiem District, Hanoi |

10. 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 (available at http://www.wellsfargo.com/privacy_security/) 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
[For Contingent Resource Staff in all countries except China, South Korea, and 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 emergency contacts). I am also aware that such processing includes conducting staff 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 engagement even after the engagement is over. I understand that that I may decline to provide the Company with my Personal Data but acknowledge that this may affect my engagement to provide services to the Company where it requires processing of my Personal Data.

By signing below, or if acknowledged electronically (e.g. by alternative modes like email, electronic signature, clicking the accept button, etc.), I hereby 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 provided them with a copy of this Notice and obtained their separate consent to their Personal Data being processed in accordance with this Notice; and
- that Personal Data I provide the Company shall be accurate and be maintained as accurate.

Legal Name (Printed)

Name of Firm (which you are employed by or work for)

Signature

Date

Acknowledgement and Consent
[For Contingent Resource Staff in the People's Republic of China]

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 emergency contacts). I am also aware that such processing includes conducting monitoring of staff 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 engagement even after the engagement is over. I understand that that I may decline to provide the Company with my Personal Data but acknowledge that this may affect my engagement to provide services to the Company where it requires processing of my Personal Data.

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 3](#) of this Notice.
- ☐ My separate consent to the provision of my Personal Data to other third parties described in [Section 3](#) 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.
- ☐ That Personal Data I provide the Company shall be accurate and maintained as accurate.

Legal Name (Printed)

Name of Firm (which you are employed by or work for)

Signature

Date

Acknowledgement and Consent [For Contingent Resource Staff in South Korea]

You understand that the Company will directly or indirectly collect, use, store, transfer (within and outside South Korea) or otherwise process your Personal Data in accordance with this Notice, and that such Personal Data includes the Personal Data of third party individuals which you provide the Company (for example, you emergency contacts). You are also aware that such processing includes conducting monitoring of staff or performing any other operations on your Personal Data.

A **summary** of what and how your Personal Data is processed is found below and **further detailed in the Notice**:

| S/N | Processing Activity | Details | | | | | | | | | | | | | | |
|---------------------------------------|--|---|-----------------------|-----------------------|----------------------|---|-----------------------|----------------------|-----------------|---------------------------------------|---------------------------------|------------------|------------------|-----------|------------------|---|
| 1 | Ordinary Personal Data Processed | Name; date of birth; CV/resume; contact information such as email address, telephone number, physical address; corporate user login ID; workstation name; IP address; software and application use records; browser history; other types of ordinary Personal Data stated in Section 1 of the Notice. | | | | | | | | | | | | | | |
| 2 | Unique Identification Information ² Processed | Currently not processed for Contingent Resource Staff in South Korea. | | | | | | | | | | | | | | |
| 3 | Sensitive Information Processed ³ | Currently not processed for Contingent Resource Staff in South Korea. | | | | | | | | | | | | | | |
| 4 | Purposes of Processing Personal Data | <ul style="list-style-type: none">Human resource management purposes in Section 2 [Paragraphs a) to c)] of the NoticeTechnology management purposes in Section 2 [Paragraph d)] of the NoticeLegal, risk and compliance purposes in Section 2 [Paragraphs e) to g)] of the NoticeCorporate restructuring purposes in Section 2 [Paragraph h)] of the NoticeHealth and safety purposes described in Section 2 [Paragraph i)] of the Notice | | | | | | | | | | | | | | |
| 5 | Period of Processing and Retention | Processing (including transfer) of Personal Data may be via electronic or physical means. Processing and retention of Personal Data will commence from the time the Vendor may be engaged to provide services to Wells Fargo and will continue until the purposes of processing are achieved, except where further retention and processing is required for exceptional reasons, such as to comply with laws or regulatory requests, or to respond to an audit, investigation or legal matter. | | | | | | | | | | | | | | |
| 6 | Transfer of Personal Data to Third Party Recipients | <table><tr><th>Transferor</th><th>Recipient</th><th>Data Transferred</th><th>Purpose of Processing</th><th>Location of Recipient</th><th>Period of Processing</th><th>Contact Details</th></tr><tr><td>Wells Fargo Bank, N.A. – Seoul Branch</td><td>Wells Fargo & Company and other</td><td>Per Item 1 above</td><td>Per Item 4 above</td><td>Worldwide</td><td>Per Item 5 above</td><td>For queries relating to Wells Fargo affiliates, please contact the South Korea Data Privacy Offer using the</td></tr></table> | Transferor | Recipient | Data Transferred | Purpose of Processing | Location of Recipient | Period of Processing | Contact Details | Wells Fargo Bank, N.A. – Seoul Branch | Wells Fargo & Company and other | Per Item 1 above | Per Item 4 above | Worldwide | Per Item 5 above | For queries relating to Wells Fargo affiliates, please contact the South Korea Data Privacy Offer using the |
| Transferor | Recipient | Data Transferred | Purpose of Processing | Location of Recipient | Period of Processing | Contact Details | | | | | | | | | | |
| Wells Fargo Bank, N.A. – Seoul Branch | Wells Fargo & Company and other | Per Item 1 above | Per Item 4 above | Worldwide | Per Item 5 above | For queries relating to Wells Fargo affiliates, please contact the South Korea Data Privacy Offer using the | | | | | | | | | | |

² Unique Identification Information refers to resident/foreigner registration numbers, passport numbers, and driver's license numbers.

³ Sensitive Information refers to information relating to an individual's race, ethnicity, ideology, belief, political opinions, admission to or withdrawal from a trade union or political party, health, sex life, DNA, criminal records, identifying physical, physiological or behavioral characteristics, and other Personal Data likely to markedly threaten their privacy.

| | | | | | | | | |
|--|--|-------------------------------------|--|--|--|--|--|--|
| | | Wells Fargo affiliates ⁴ | | | | | details in Section 8 of the Notice | |
|--|--|-------------------------------------|--|--|--|--|--|--|

You acknowledge that this Notice and this ‘Acknowledgement and Consent’ form will supersede any prior notice on this subject and shall cover all Personal Data collected or maintained by the Company in connection with your engagement even after the engagement is over.

Having reviewed this Notice and this ‘Acknowledgement and Consent’ form, **please provide your consent** to the processing of your Personal Data by **completing, signing and checking all boxes the form below.**

Providing your consent is voluntary. However, if consent is not provided, Wells Fargo may not be able to engage you and the Vendor to provide services where such services require the processing of your Personal Data.

| | |
|---|---|
| Your consent to collection and processing of your Ordinary Personal Data in accordance with this Notice. | I consent <input type="checkbox"/> |
| Your consent to provision of your Ordinary Personal Data to third party recipients described in Section 3 of this Notice. | I consent <input type="checkbox"/> |
| Your consent to your Personal Data being transferred to recipients outside South Korea as described in this Notice after having reviewed the implications of such overseas transfers as described in Section 3 of this Notice. | I consent <input type="checkbox"/> |
| Where you provide Personal Data of other third party individuals to Wells Fargo, that you 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. | I acknowledge and confirm <input type="checkbox"/> |
| That Personal Data you provide the Company shall be accurate and maintained as accurate. | I acknowledge and confirm <input type="checkbox"/> |

| | |
|----------------------------|--|
| <hr/> Legal Name (Printed) | <hr/> Name of Firm (which you are employed by or work for) |
| <hr/> Signature | <hr/> Date |

⁴ Wells Fargo has affiliated entities operating in the United States (US) and around the world, including the Wells Fargo group parent in the US, Wells Fargo & Company. Non-exhaustive lists of affiliated entities can be found in the Wells Fargo & Company 10-K filings made with the US Securities and Exchange Commission, found at the following hyperlinks:
 (List 1) <https://www.sec.gov/Archives/edgar/data/72971/000007297125000066/wfc-1231x2024xex21.htm>; and
 (List 2) <https://www.sec.gov/Archives/edgar/data/72971/000007297115000449/wfc-12312014xex21.htm>

Acknowledgement and Consent
[For Contingent Resource Staff in Vietnam]

I understand that the Company will directly or indirectly collect, use, store, transfer (within and outside Vietnam) 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 emergency contacts). I am also aware that such processing includes conducting monitoring of staff 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 engagement even after the engagement is over. I understand that that I may decline to provide the Company with my Personal Data but acknowledge that this may affect my engagement to provide services to the Company where it requires processing of my Personal Data.

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

- ☐ My separate consent for my Personal Data to be collected and processed in accordance with this Notice for the human resource including vendor management purposes described in [Section 2](#) [Paragraphs a) to c)] of the Notice.
- ☐ My separate consent for my Personal Data to be collected and processed in accordance with this Notice for the technology management purposes described in [Section 2](#) [Paragraph d)] of the Notice.
- ☐ My separate consent for my Personal Data to be collected and processed in accordance with this Notice for the legal, risk and compliance purposes described in [Section 2](#) [Paragraphs e) to g)] of the Notice.
- ☐ My separate consent for my Personal Data to be collected and processed in accordance with this Notice for the corporate restructuring purposes described in [Section 2](#) [Paragraph h)] of the Notice.
- ☐ My separate consent for my Personal Data to be collected and processed in accordance with this Notice for the health and safety purposes described in [Section 2](#) [Paragraph i)] of the Notice.
- ☐ My separate consent for my Personal Data to be transferred to recipients outside Vietnam as described in this Notice after having reviewed the implications of such overseas transfers as described in [Section 3](#) of this Notice.
- ☐ 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.
- ☐ That Personal Data I provide the Company shall be accurate and maintained as accurate.

Legal Name (Printed)

Name of Firm (Which you are employed by or work for)

Signature

Date