
Wells Fargo Apprentice Privacy Notice

This Notice applies to Apprentices in India

Effective: 01 July 2025

The Wells Fargo entity which has engaged the vendor organization that engaged you ("**we**", "**us**", "**our**" or the "**Company**") provides this Privacy Notice ("**Notice**") to explain how the Company will Process your Personal Data, Wells Fargo's privacy practices, and your rights over your Personal Data. 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 information directly or indirectly identifying you or individuals relating to you ("**Personal Data**").

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 your engagement, including administering your contract or engagement relationship with the Company, we need to collect, process, and use Personal Data. We also 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 Officers are listed below in [Section 8](#).

1. What Personal Data Do We collect?

The vendor may collect and transfer to us, or we may collect the following categories of Personal Data in connection with your engagement:

- **Master data:** such as name (first name, last name, family name), date of birth, 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.
- **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.
- **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) footages/video and audio surveillance equipment installed according to local law onto Wells Fargo business premises; information about your location; office access data;
- **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, 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:** 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.
- **Sensitive Personal Information:** We may also collect from you certain types of sensitive Personal Information, such as physical or mental health information, as permitted by local law, for example, in relation to disability accommodations, or such as sensitive data contained in communications such as email that are reviewed in the course of risk management activities.

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. 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 administer our engagement with the Vendor where it requires the processing of your Personal Data.

2. Why We Process Your Personal Data

The Company process the types of Personal Data listed in Section 1 for the following purposes (collectively “**Engagement Purposes**”).

- a) **Human resource management purposes relating to handling, maintaining, and improving administration of our engagement 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; determining and managing your suitability to be engaged for present or future engagements; maintaining internal lists or databases relating to your suitability for engagement. For this purpose, the Company may process Master data, work contact details, visa and work permit 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, sensitive personal data and other categories of Personal Data where needed.
- d) **Technology management purposes.** For example: implementing, maintaining, and upgrading Information Technology (IT) systems; 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 and ensuring compliance with the Wells Fargo Code of Ethics and Business Conduct, other policies and procedures, and applicable laws.** 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; preventing fraud and other illegal activities; 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, a, 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 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, 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.
- j) **To determine your suitability to be engaged,** at the time Vendor assigns you to Wells Fargo for job training that requires access to Wells Fargo's network to determine whether you appear on Wells Fargo's and its affiliates' "Do Not Hire" or "Do Not Reengage" lists or to place your Personal Data on the Wells Fargo and affiliates' "Do Not Hire" or "Do Not Reengage" lists, if Wells Fargo determines, in its discretion, that you have committed a crime involving theft, fraud or dishonesty or committed a serious violation of Wells Fargo's code of conduct or information security policies, and maintain the Personal Data on such lists for purposes of future consultation, Company may process master data and disciplinary data.

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 Employment Purposes described in [Section 2](#).

We have put in place measures to enable the transfer of Personal Data to another country in accordance with applicable law regardless of the global location of our entities. These measures enable us to transfer and use Personal Data in a secure manner anywhere in the world where we have operations, or where we have contracted third parties to provide us with services.

- **Wells Fargo U.S.** Since management, human resources, legal and audit responsibility partially rests with Wells Fargo & Company as the group parent in the United States ("**Wells Fargo & Company**") and with Wells Fargo Bank, N.A. operations in the U.S. ("**Wells Fargo Bank, N.A.**") (collectively, "**Wells Fargo U.S.**"), the Company may transfer Personal Data to, or otherwise allow access to such data by, Wells Fargo U.S., which may use, transfer, and process the data for the following purposes: to maintain and improve effective administration of the workforce; to provide rights, benefits, stock grants, and entitlements; to maintain a corporate directory; to maintain IT systems; to monitor and assure compliance with Wells Fargo's Code of Ethics and Business Conduct, other policies and procedures, and applicable law; and to respond to requests and legal demands from regulators and other authorities, including such authorities in the United States.

- **Affiliated Entities.** To the extent that your management or human resources responsibility for overseeing your employment relationship with the Company partially rests with different Wells Fargo entities ("**Affiliated Entities**"), the Company may also transfer Personal Data to, or otherwise allow access to such data by, relevant Affiliated Entities, which may use, transfer, and process the data for the following purposes: to maintain and improve effective administration of the workforce; to provide rights, benefits, stock grants, and entitlements, to maintain a corporate directory; to maintain IT systems; to monitor and assure compliance with Wells Fargo's Code of Ethics and Business Conduct, other policies and procedures, and applicable law; and to respond to requests and legal demands from regulators and other authorities, including authorities in the jurisdictions where the Affiliated Entities are located. The current Wells Fargo & Company 10-K filing, Exhibit 21, made with the US Securities and Exchange Commission provides a non-exhaustive list of the Affiliated Entities.
<https://www.sec.gov/Archives/edgar/data/72971/000007297125000066/wfc-1231x2024xex21.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, 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 Employment Purposes 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 the Company will generally have access to your business contact information such as 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.

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

The Company's general practice is not to keep Personal Data longer than necessary for the fulfillment of the Engagement Purposes outlined in [Section 2](#), in accordance with our standard records retention periods, or as required or appropriate in the jurisdiction where such records or information is retained. However, we and our service providers may need to hold Personal Data beyond these time periods for reasons such as complying with the regulatory requirements of a particular country or in response to an audit, investigation, or other legal matter. The criteria used to determine retention periods include but are not limited to:

- 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; 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.

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 over your Personal Data which is processed by the Company, such as the following:

- Right to request for: (i) a summary of personal data processed, and the processing activities undertaken by the Company; and (ii) the identities of data recipients with whom personal data has been shared and a description of the personal data shared with such recipients.
- Right to correct, complete, update, and erase your Personal Data.
- Right to withdraw consent given to processing of your Personal Data. Such withdrawal will not affect the lawfulness of processing performed prior to the withdrawal, or processing based on lawful grounds other than consent.
- Right to nominate any other individual who, in the event of your death or incapacity, can exercise your rights. • Right to have your grievances redressed.
- Right to request for the contents of this Notice to be provided in any language specified in the Eight Schedule to the Constitution of India.

The above mentioned rights may not be absolute and may vary or be subject to exceptions or limitations. If the Company is not able to accommodate your request, you will be provided with reasons for the denial. We will respond to a written complaint within 30 days. If you are not satisfied with our response, you may be able to pursue your complaint with your data protection authority or privacy commissioner for your country. If you wish to seek redress for grievances relating to the processing of your Personal Data, please contact the India Grievance Officer using the contact information in Section 8 below.

8. Contacting Us For Your Request

The Company has appointed the Grievances Officer (as listed below) who is responsible for responding to requests in relation to your Personal Data.

Wells Fargo International Solutions Private Limited

Vijayalakshmi Kannan

Vijayalakshmi.Kannan@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.

Acknowledgement and Consent

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