

---

# Wells Fargo International Employee Privacy Notice

This Notice applies to employees in India and the Philippines, except employees of Wells Fargo Bank, N.A. – Mumbai, India.

**Effective:** 03 April 2026

"**We**", "**Our**" or "**Company**" refers to the Wells Fargo entity with which you have an employment contract, and which is acting as the data controller regarding the collection, use, storage, deletion, transfer, and processing of individually identifiable information relating to you ("**Personal Data**"). "**You**" or "**your**" refers to an individual who has an employment contract or employment 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. We also have to meet the different requirements of data protection laws across the world. If you are employed by a different Wells Fargo entity, a different privacy notice will govern your employing entity's Personal Data collection and processing activities.

**Name of group parent:** Wells Fargo & Company

**Headquarters location:** 333 Market Street; San Francisco, CA 94105 USA

Contact information for our designated Officers are 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:** 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, sex (male/female), national identification or documents issued by a governmental authority, tax, and/or social benefits and/or insurance number, information required for tax reporting, health insurance information, death information (i.e. death certification information) of employees or dependents, signature, photograph, bank account, and corporate credit card details
- **Background data:** credit history, professional qualifications or licenses, previous addresses, prior employment history, ownership and/or proprietorship current and past directorships held by you and members of your immediate family, education history and professional or personal references, educational background (college, university, location, major, year of entrance and year of graduation, graduation status, GPA, etc.), career (company, title, responsible duties, service period), resume, qualifications and professional or personal references.
- **Visa and work permit data:** copies of your passport, birth certificate, national identification card, existing and

expired visa(s) and other permit details, and all such information for relevant members of your family (such as your parents, spouse, domestic/civil partner, children and/or other dependents), if required by applicable law.

- **Emergency contact information:** first name, family name, and contact information of a family member or other person to be contacted in an emergency.
- **Work contact details:** work address, work phone numbers, fax numbers, and work email address.
- **Contract data:** 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:** 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:** data that may be collected in the course of employment including business travel, business expenses, use of Company facilities, use of onsite clinic, employee referral, press articles, social media content, employee branding materials, training activity, attendance, photographs and videos at Company events.
- **Computer/Device usage and monitoring data and contents:** data about when and how you use and interact with equipment, software applications, electronic communications systems, 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, CCTV footages or recordings, intranet SharePoint sites, shared drives and other data repositories, voicemail, and software (including software you install), and how your use compares with benchmarks based on both your own prior use and others' use, and risk-rating scores based on such use.
- **Performance data:** performance evaluations, appraisals, promotions, coaching journals and assessments of performance.
- **Disciplinary data:** information about conduct, investigations, and disciplinary notices, if any.
- **Absence data:** dates of absence and reasons for absence (such as medical leave) to the extent these apply to you.
- **Benefits information:** car, mobile device, gym/fitness and housing allowance, contribution to health insurance, pension contribution, and company provided transportation the name, address, gender, and date of birth of your spouse or domestic civil/partner, and/or dependents or children who are beneficiaries (if applicable).
- **Bonus and incentive information:** details of applicable bonus, incentive and commission plans.
- **Third party data:** 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 information on medical reports, medical questionnaires, employee health reviews and vaccines plans, food restrictions and food choices, workplace illness and accidents, data about sick leave processed in the course of existing employment and relevant for payroll 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 travel, 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, hand scans, biometric algorithms, voice prints and facial recognition
- **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 or compliance activities.

Amongst the types of Personal Data listed above, some of them may constitute Personal Data which is considered sensitive under applicable privacy laws ("**Sensitive Personal Data**"). Under the respective privacy laws Sensitive Personal Data is Personal Data relating to some or all of the following types of information: (i) passwords; (ii) financial information such as details of bank account/credit card/debit card/other payment instruments; salary or payslips, certificate of employment which includes salary information; personal income tax documents (iii) an individual's health, education, genetic traits, or sexual life; (iv) sexual orientation; (v) medical records and history; (vi) biometric data such as fingerprints, hand scans, biometric algorithms, voice prints and facial recognition; (vii) race, ethnic origin, marital status, age, colour, and religious, philosophical, or political affiliations (viii) criminal records, offenses (alleged or actual) and proceedings; (ix) information issued by government agencies peculiar to an individual such as social security numbers; and (x) information specifically established by an executive order or act to be kept classified.

If you, for any purpose under this Notice, provide the Company with Personal Data about your spouse/domestic/civil/partner, dependents and/or dependent minors as their parent or legal guardian (for example, for emergency contact or for benefits administration purposes) or other third parties, it is your responsibility to inform them of their rights with respect to such Personal Data and that you may disclose their Personal Data to the Company for these purposes. You are also responsible for obtaining the explicit consent of these individuals (unless you are authorized to provide such consent on their behalf) if such consent is required by applicable law for the collection, use, storage, transfer and processing of their Personal Data. 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 Privacy Notice and Pursuant to applicable law.

The Company must collect your Personal Data, without which we will not be able to process your Personal Data for the purposes set out in Section 2 below, and the administration of your employment, including the Employment Purposes (defined below), could be affected.

## 2. Why We Process Your Personal Data

The Company uses and processes Personal Data (via manual and electronic methods) for the following purposes (collectively, "**Employment Purposes**"), as permitted by applicable law.

- **To provide 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 data, bonus and incentive information, performance data, absence data, disciplinary data, diversity-related data, Sensitive Personal Data, and benefits information, for example.
- **To provide 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, and visa and work permit data, for example.

- **To comply with other employment-related legal requirements**, such as income tax, national insurance deductions, health monitoring/declaration to government agencies (i.e., due to pandemic) and applicable employment and immigration laws and other specific legal requirements for certain roles. 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, Sensitive Personal Data, and absence data, for example.
- **To maintain and improve effective administration of the workforce and company facilities.** For example: assigning projects and tasks, making business travel arrangements, international assignments; making transport arrangements, mail dispatches, managing business expenses and reimbursements; managing and administering vacation and leave time, office time, conducting workforce analysis, administering project costing and estimates, managing work activities, employee volunteering or Corporate Social Responsibility activities, industry conferences and events, providing performance evaluations and promotions, conducting talent management, succession planning, opinions expressed when participating in surveys; designing performance improvement or employee retention programs; and career development, 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), and providing facilities management and worksite physical access and security. For this purpose, the Company may process Personal Data such as master data, work contact details, organizational data, employment data, contract data, performance data, absence data, disciplinary data, diversity-related data, and Sensitive Personal Data, for example.
- **To maintain a corporate directory and offer platforms for sharing information.** For example: populating and making available contact details and/or an intranet website accessible by Company employees and authorized contingent resources to facilitate communication with you or sharing of information internally. For this purpose, the Company may process Personal Data such as work contact details, organizational data, and other data you voluntarily submit for these purposes.
- **Technology management purposes.** For example: implementing and maintaining Information Technology ("IT") systems, providing IT support and asset management, enhancing systems and applications, maintaining business continuity and recovery plans and processes, and not limited to adoption of alternative and/or flexible work arrangements and managing security services and employee access rights, identity, 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, computer usage data, organizational data, Sensitive Personal Data, personal data contained in communications, and disciplinary data, for example.
- **Legal, risk, and compliance purposes relating to monitoring and ensuring compliance with the Wells Fargo's Code of Ethics and Business Conduct, other policies and procedures, and applicable law.** For example: detecting or preventing possible loss or unauthorized access or processing of customer, employee, confidential or restricted data, protecting Company and other party data and assets, mitigating insider trading risk, avoiding actual or perceived conflicts of interest, and meeting regulatory expectations, conducting internal audits and investigations, handling any potential or other claims, address grievance 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, personal data contained in communications, Sensitive Personal Data, computer usage data, and disciplinary data, for example.
- **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 claim or proceeding involving any Wells Fargo entity.** For example: complying with requests from regulators or other authorities in your home country or other jurisdictions, such as attachment of earnings orders, and participating in legal proceedings including domestic and

cross-border litigation and discovery procedures, and where permitted or required by law, disclose to third parties such as the police and/or other law enforcing authorities without employee consent. For this purpose, the Company may process Personal Data such as work master data, contact details, organizational data, contract data, bonus and incentive information, performance data, background data, third party data, Sensitive Personal Data, computer usage data, personal data contained in communications, disciplinary data, employment data, and any other category of Personal Data necessary to respond to the request or legal demand,

- **To notify you or your family or emergency contacts in the event of any emergencies.** Such as, providing support during emergency and protecting the health and safety of employees and others, and protecting office equipment, facilities and other property. For this purpose, the Company may process Personal Data such as master data and emergency contact information, for example.
- **To perform certain limited activities with respect to Sensitive Personal Data,** including calculating the number of sick days for statutory wage tracking, reporting workplace accidents as required by applicable law, complying with obligations to make reasonable adjustments and complying with regional legislation and anti-discrimination policies, monitoring/reporting of equality of opportunity and treatment generally amongst our staff (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, and reviewing our interviewing and hiring processes and our pay and conditions), confirming someone's right to work, verifying identity for security and fraud prevention purposes, and complying with other applicable law. For this purpose, the Company may process Personal Data such as Sensitive Personal Data, master data, and diversity-related data, for example.
- **To promote public health and to ensure workplace health and safety,** such as in connection with the COVID-19 pandemic, where permitted or required by applicable law, the Company may process Personal Data such as certain sensitive health and recent travel information, which may include but not be limited to body temperature, symptom, recent travel, potential or confirmed exposure, testing (including results), and/or vaccination information, and Sensitive Personal Data, for example.
- 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.
- **Advanced Automated Systems and Processing.** For example, analyze information, enhance the accuracy of our operations, support the delivery of efficient and personalized services, and use of technologies to help identify patterns, assess risks, detect potential security concerns, streamline workflows, and improve overall service quality. For this purpose, the Company may process personal data such as master data, work contact details, performance data, absence data, engagement data, usage and monitoring data, and other categories of Personal Data where needed.
- **Use of Artificial Intelligence and Automated Tools:** We may use automated tools, including artificial intelligence and limited profiling, to support organizational, Human Resources and workplace activities. These tools may analyse information to assist decisionmaking, but do not make decisions on their own that have legal or similarly significant effects on employees, unless permitted by law. We use human oversight and appropriate safeguards to assess outcomes and make final decisions.
- 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 6 below for further information about how long we retain Personal Data.

In order to fulfill any of the Employment Purposes, it may be necessary for the Company to carry out, in whole or in part, automated decision-making operations or profiling. This automated process may be the sole basis for a decision which may produce a legal effect. By attesting to or signing this Privacy Notice, you consent to the processing of your Personal Data

through this automated processing system. In the event of such processing, the Company shall notify the Data Privacy Authority such processing system in accordance with applicable laws and regulations and will ensure that there are safeguards against the harms of extensive profiling.

### 3. Transfers of Your Personal Data to other Recipients

Wells Fargo operates across the globe, and we may transfer Personal Data for Employment Purposes to Wells Fargo entities located in other countries. This can also happen when we engage third parties to assist us with certain operations and activities, as they also may be established in different countries.

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. We may also transfer Personal Data to other countries where our third-party service providers are located.

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 not be limited to your managers and their designees, and personnel in HR, IT, Compliance, Legal, Finance, Chief Operating Office 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, postal address, and email address.

The Company may transfer Personal Data (including Sensitive Personal Data) to the following third parties for the Employment Purposes:

- **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. The list as of December 31, 2025 is found at: <https://www.sec.gov/Archives/edgar/data/72971/000007297126000133/wfc-1231x2025xex21.htm>
- **Customers and Prospects.** As necessary in connection with business operations, work contact details may be transferred to customers and other third parties as permitted by applicable law.
- **Regulators, authorities, and certain third party controllers.** As necessary for the Employment Purposes described above, Personal Data may be transferred to regulators, courts, and other authorities (e.g., tax and law enforcement authorities), other partner organizations and the Wells Fargo & Company Board of Directors.
- **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 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 ("**Data Processors**"). Such Data Processors may carry out instructions related to IT system support, HR services payroll, training, compliance, and other legitimate activities or purposes, and will be subject to contractual obligations to implement appropriate technical and organizational security measures to safeguard the Personal Data, and to process the Personal Data only as permitted by the contract. In addition, to the extent that Personal Data is disclosed to independent external auditors, benefits providers, insurance carriers, other service providers, or other partner organizations that may not be acting solely as a Data Processor, such service providers will be subject to any necessary contractual obligations regarding the protection and processing of such information. Please refer to the booklet available by request listing the third parties to which Personal Data is transferred for processing and a description of that processing

The recipients of Personal Data identified in this Section 3 may be located in the United States and other jurisdictions that may not provide the same level of data protection as your home country. To the extent required by applicable law, the Company, Wells Fargo U.S., and Affiliated Entities will: (i) address any applicable requirement to assure an adequate level of data protection before transferring Personal Data by assuring the execution of appropriate data transfer agreements or confirming other controls or otherwise provide appropriate safeguards regarding transfers of Personal Data to other countries; and (ii) establish that Personal Data will be made available to individuals within the recipient entities on a need-to-know basis only for the relevant Employment Purposes described above and as necessary for the fulfillment of its obligations under this privacy notice (collectively, the "**Safeguards**"). In addition, if certain circumstances as applicable under privacy law apply, the identities of recipients of Personal Data under the above-mentioned data transfer agreements may be made available upon request. Please contact the Officer, using the contact information in Section 8, to obtain additional information about these Safeguards or to make such a request.

## 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. 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. Exercising Your Rights Over Your Personal Data.

You may have certain rights under applicable law that enable you to have control and oversight over what organizations do with your Personal Data. These rights may include the right to be informed, request access, correct, suspend use, portability, delete, object, right to damages, nominate, or grievance redressal, related to the processing of your Personal Data. You may also have the right to withdraw any consent previously given, but such withdrawal will not affect the lawfulness of processing done prior to your withdrawal, or processing conducted on legal bases other than consent. These rights are not absolute, and exceptions may apply. If we are not able to accommodate your request, you will be provided with reasons for the denial. If you have questions about your Personal Data rights, or whether different local laws apply, please contact the applicable Officer listed in Section 8 below.

You may have the right to file a complaint with the Data Protection Authority for your country if you feel actions taken by

us or our employees violate your rights under applicable law and you are not satisfied with the resolution we provide. Contact information for the Data Protection Authority in the Philippines is available at: <https://www.privacy.gov.ph/>.

## 6. How Long Is Your Personal Data Retained

We will retain your Personal Data for so long as we are required to do so by applicable laws and for as long as necessary for the purposes of use and processing described in [Section 2](#). We and our third-party service providers maintain Personal Data during your engagement with us and for legal, regulatory, audit, or legitimate business reasons. Factors for determining data retention may include the length of your engagement, legal obligations, litigation/regulatory needs, and operational requirements. Retention schedules are maintained internally and applied by record type and jurisdiction.

## 7. 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 equipment, electronic communication 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, computer use activity, and CCTV. 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 assure compliance with Wells Fargo's Code of Ethics and Business Conduct, and other Company policies and procedures. You should not expect privacy in connection with your use of any equipment, systems, or property, including personally owned equipment to the extent subject to Company Bring Your Own Device ("**BYOD**") policies. Wells Fargo also maintains separate policies that govern BYOD, including when and how Wells Fargo may perform monitoring. If you use a BYOD approved device, you should review those policies.

Even if you create or have access to passwords to protect against unauthorized access to correspondence and activities, using that password does not make the related communications or activities private. In addition, phone calls, video calls, and/or instant messages or chats made or received on any business telephone or any Company device may be monitored or recorded for regulatory and compliance purposes. Monitoring may be conducted remotely or locally, and related Personal Data collected and processed by the Company, Wells Fargo U.S., Affiliated Entities, and/or Data Processors using software, hardware or other means. Personal Data obtained through monitoring may be transferred to regulators and other authorities, as well as the Wells Fargo & Company Board of Directors, and other recipients as necessary for the purposes described above, including recipients in your home country or other jurisdictions. Personal Data obtained through monitoring will be safeguarded in accordance with the security measures set out in Section 4 above. Personal Data obtained through monitoring, which is relevant to the purposes described above, will be retained for the time periods described in Section 6 above subject to any rights employees may have under applicable law.

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 pursuant to Section 6 above, and subject to any rights employees may have under applicable law

## 8. Who To Contact With Questions Your Personal Data

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

**India:**

Wells Fargo International Solutions Private Limited  
Wells Fargo Centre, Building 1A,  
Divyasree NSL SEZ Survey No. 66/1,  
Raidurga Village, Serlingampalli,  
Hyderabad, Telangana 500032)  
[IP.privacy@wellsfargo.com](mailto:IP.privacy@wellsfargo.com)

**Philippines Data Protection Officer:**

Wells Fargo International Solutions LLC – Philippines and  
Wells Fargo International Clearing Support Services, LLC –  
Philippine Branch  
Data Protection Officer (DPO)  
1180 Wells Fargo Drive,  
McKinley Hill, Dr. Taguig, Philippines  
[IP.Privacy@wellsfargo.com](mailto:IP.Privacy@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. National Privacy Commission (NPC) seals of Registration

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 at the following [link](#).

### Acknowledgement and Consent

By signing or clicking the accept button, or if acknowledged electronically (e.g., by alternative mode like email, electronic signature, etc.), I 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 with the full knowledge of the implications of such overseas transfers as described in Section 3 of this notice;
- I have informed third party individuals that I provide Personal Data to the Company of the terms of this Notice and obtained their separate consent to their Personal Data processed in accordance with this Notice;
- 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 the Personal Data that I provide the Company shall be accurate and be kept accurate.

---

Legal Name (Printed)

---

Signature

---

Date