
South Korea

Wells Fargo International Employee Privacy Notice

Effective: 05 June 2025

Wells Fargo Bank, N.A. Seoul Branch ("**we**", "**us**", "**our**" or the "**Company**") provides this privacy notice ("**Notice**") to describe its practices regarding the collection, use, disclosure, and other processing of individually identifiable information directly or indirectly identifying you or individuals relating to you ("**Personal Information**") in relation to your employment or service relationship with the Company. The Company acts as the data controller regarding the collection and processing of your Personal Information.

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 and employment relationship with the Company, we need to collect, process, and use Personal Information during and after employment. We also have to meet the different requirements of data protection laws across the world. This Notice covers Wells Fargo entities in South Korea. If you are employed by a Wells Fargo entity in any country other than South Korea, a different privacy notice will govern that entity's Personal Information collection and processing activities.

Name of group parent: Wells Fargo & Company

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

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

1. What Personal Information Do We Collect?

We may collect the following categories of Personal Information in connection with your employment:

- **Master data:** such as 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), government-issued identification information (such as Resident / Foreigner Registration Numbers, passport information, driver's license, etc.), national tax and/or social benefits, housing fund and/or insurance number, information required for tax reporting and withholding, basic insurance information for employees, family members and/or dependents, photograph, bank account details, etc.
- **Background data:** such as credit history, professional qualifications, previous addresses, prior employment history, previous and current ownership and/or proprietorship current and past directorships held by you and members of your immediate family, education history, and professional or personal references, 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, history of awards, date of employment, department, title, duties, etc.
- **Visa and work permit data:** such as copies of your passport, birth certificate, government-issued identification information, 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), etc.

- **Emergency contact information:** such as name and contact information of a family member or other person to be contacted in an emergency, etc.
- **Work contact details:** such as name, work address, work phone numbers, fax numbers, work email address, etc.
- **Contract data:** such as terms and conditions of your contract, salary or pay, and other contractual benefits such as car, educational or housing allowances; stock, incentive, or bonus awards; and changes to the terms and conditions of your employment or work relationship, etc.
- **Organizational data:** such as title, job position, function, employee ID, department, business unit, supervisor's name and higher level supervisor(s), cost center, signing authority, skills, work experience at the Company, user ID, information technology access rights, etc.
- **Employment data:** such as data that may be collected in the course of employment including business travel, business expenses, use of Company facilities, training activity, attendance at Company events, etc.
- **Performance data:** such as performance evaluations, appraisals, promotions, assessments of performance, etc.
- **Disciplinary data:** such as information about conduct, investigations, disciplinary actions, and disciplinary notices, if any.
- **Absence data:** such as dates of absence and reasons for absence (such as medical leave) to the extent these apply to you.
- **Benefits information:** such as car, mobile device, gym/fitness and housing allowance, contribution to health insurance, stock option plan details, pension contribution, and the name, address, gender, and date of birth of your spouse or domestic civil/partner, and/or dependents or children who are beneficiaries (if provided by you), etc.
- **Bonus and incentive information:** such as details of applicable bonus, incentives, commission plans, etc.
- **Third party data:** such as the name, title, employer, contact details, and location of any individual who you are related to or have a close personal relationship with who: (i) provided you with a reference for employment with Wells Fargo; (ii) is a U.S. or non-U.S. government official; or (iii) has decision making authority/capability over any matters affecting Wells Fargo, and any other Personal Information relating to another individual which you may provide or disclose directly/indirectly to the Company.
- **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), etc.
- **Usage and monitoring data:** such as data about when and how you use and interact with equipment, electronic communications systems, software (including those you install), and property, such as computers, mobile devices, email, internet, geolocation, calendar invitations, shared files, instant message or chat, video and/or audio calls, recordings and transcriptions, internet, SharePoint, shared drives and other data repositories and voicemail, and how your use of the above compares to others to create benchmarks and risk-rating scores based on such use; images and voices about you that may be captured by closed-circuit television (CCTV) video and audio surveillance equipment installed according to local law onto the Company's business premises; office access data; device data relating to personal electronic devices or other equipment used for any Bring Your Own Device program, e.g. device OS or model.
- **Personal Information contained in communications:** such as the types of Personal Information listed above that may be contained in emails, phone calls, video calls, and/or instant messages or chats made or received on any business telephone or any Company device or other means of communication that are reviewed in the course of risk management, compliance, and other employment or business activities.

- **Criminal records data:** such as criminal records properly obtained through a lawful background reference check.
- **Diversity-related data:** such as race, ethnicity, gender identity, sexual orientation, veteran/military status, disabilities, and personal pronouns.
- **Biometric data:** such as fingerprints, keystrokes, hand scans, biometric algorithms, or voice prints.
- **Health-related data:** such as information on medical reports, medical questionnaires, employee health reviews and vaccines plans; health-related data in connection with processing and management of leave, absence, tax, workplace illness and accidents, workplace health and safety, disability access, pregnancy; data relevant to public health (e.g. body temperature, symptoms, recent travels, potential or confirmed exposure, testing (including results), and vaccination status); health-related data where required or requested by law, regulation or regulators (for example, in connection to managing health pandemics like COVID-19).

Amongst the above Personal Information, some of them are considered under privacy laws in South Korea as:

- **unique identification information**, which refers to passport numbers, driver's license numbers, resident/foreigner registration numbers, and other government-issued identification information.
- **sensitive information**, which refers to information relating to an individual's ideology, belief, admission to or withdrawal from a trade union or political party, political opinions, health, sex life, DNA, criminal records, biometrics, and other personal information that is likely to markedly threaten the privacy of that individual.

Unless stated otherwise, references to Personal Information in this Notice include unique identification information and sensitive information. However, the collection, use, disclosure, and processing of such information shall only be done where necessary to achieve the purposes described in [Section 2](#) and to the extent permitted by law.

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

We will process your Personal Information 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 Information (including unique identification information and sensitive information), without which we will not be able to process your Personal Information for the Employment Purposes in [Section 2](#), and the administration of your employment be affected where it requires the processing of your Personal Information.

2. Why We Process Your Personal Information?

The Company processes the types of Personal Information listed in [Section 1](#) to carry out the employment relationship with you and its business operations, and for the following purposes ("**Employment Purposes**").

- **Human resource management purposes relating to providing compensation.** For example, managing payroll, bonus, stock options, and incentives as applicable. For this purpose, the Company may process Personal Information such as master data, contract data, bonus and incentive information, performance data, absence data, disciplinary data, benefits information, and other categories of Personal Information where needed.

- **Human resource management purposes relating to providing rights, benefits, rewards, recognition, awards, company events and entitlements, and other conditions as applicable.** For this purpose, the Company may process Personal Information such as master data, work contact details, organizational data, contract data, bonus and incentive information, performance data, absence data, disciplinary data, benefits information, employment data, diversity-related data, visa and work permit data, and other categories of Personal Information where needed.
- **Human resource management purposes relating to handling, maintaining, and improving administration of the workforce and business operations.** For example: assigning projects and tasks; making business travel arrangements; managing business expenses and reimbursements; managing and administering vacation and leave time, and office time; conducting workforce analysis; administering project costing and estimates; facilitating and managing work activities relating to customers and other third parties dealing with the Company and other Wells Fargo entities; providing performance evaluations and promotions; conducting talent management and career development; succession planning; designing employee retention programs; providing references as requested (if permitted by Company policy); administering learning and development training (including approaching you to suggest specific training or gauge your interest in participating in a mentoring programme); providing workplace disability support; supporting veteran initiatives; where you provide your Personal Information to engage or participate in diversity monitoring initiatives, your Personal Information may be used to support monitoring and reporting of equality of opportunity and treatment generally amongst staff ("**Diversity Monitoring**"), including in relation to: facilitating diversity, equality and inclusion efforts, reviewing processes concerning the promotion of staff and appointment of senior personnel within the business, reviewing interviewing and hiring processes including in order to take action when someone with a specific characteristic suffers a disadvantage, and reviewing pay and conditions; conducting employee surveys; supporting business continuity and recovery and resolution planning efforts; supporting alternative and/or flexible work arrangements; providing management and security of facilities, worksites and systems; and verifying identity for security purposes. For this purpose, the Company may process Personal Information such as master data, work contact details, organizational data, contract data, performance data, health-related data, absence data, employment data, diversity-related data, disciplinary data, biometric data, and other categories of Personal Information where needed.
- **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 Company staff, in order to facilitate staff communication and sharing of information internally. For this purpose, the Company may process Personal Information such as work contact details, organizational data, other data you voluntarily submit for these purposes, and other categories of Personal Information where needed.
- **Human resource management purposes in the event of emergencies,** such as contacting you, your family or emergency contacts, protecting the health and safety of employees and others in emergencies, and protecting office equipment, facilities, and other property. For this purpose, the Company may process master data, emergency contact information, and other categories of Personal Information where needed.
- **Technology management purposes.** For example: implementing, maintaining and upgrading information, cloud, artificial intelligence and other technology systems, applications, features or services; maintaining business continuity and recovery plans and processes; supporting the adoption of alternative and/or flexible work arrangements; managing security services; managing employee access to systems and equipment; compiling of audit trails and other reporting tools; and identifying patterns in the use of technology systems and information entrusted to us to protect Company, people and property. For this purpose, the Company may process Personal Information such as master data, work contact details, usage and monitoring data, organizational data, Personal Information contained in communications, disciplinary data, and other categories of Personal Information where needed.
- **Legal, risk and compliance purposes relating to monitoring, investigating, and supporting compliance with Wells Fargo's policies and procedures as well as laws, regulations, regulatory guidance and expectations, and**

codes of practice relating to Wells Fargo and its customers, prospects or counterparties. For example: detecting or preventing possible loss or unauthorized access or processing of customer, employee, confidential or restricted data; protecting Company, customer and third party data and assets; managing and mitigating risk; preventing fraud and other illegal activities; avoiding actual or perceived conflicts of interest; meeting regulatory expectations; conducting internal audits and investigations; complying with obligations to make reasonable adjustments and complying with regional legislation and anti-discrimination policies, ensuring compliance with internal HR and Return to Office policies; handling any potential complaints or other claims; and engaging in disciplinary actions and terminations. For this purpose, the Company may process Personal Information 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, usage and monitoring data, and disciplinary data, Personal Information contained in communications, and other categories of Personal Information where needed.

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

The Company will not process Personal Information 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 Information continues after individuals have left the service of the Company. Please see [Section 4](#) below for further information about how long we retain Personal Information.

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

3. Transfers of Your Personal Information to other Recipients

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

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

The recipients of Personal Information 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 Information. 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 Information by ensuring the execution of appropriate data transfer agreements or confirming other reasonable safeguards are in place; and (ii) establish that Personal Information will be made available to recipients on a need-to-know basis only for the Employment Purposes described above. These data transfer safeguards enable us to transfer and use Personal Information in a secure manner anywhere in the world where we have an establishment, or where we have contracted third parties to provide us with services.

Personal Information may be transferred electronically (e.g., by IT network, etc.) or physically (e.g., by courier, post, etc.) during your employment 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 Information.

4. How We Safeguard Your Personal Information

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

- 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 security and control standards, and perform periodic third-party risk assessments.

5. Retention and Destruction of Personal Information

Retention of Personal Information

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

- The length of time we have an ongoing relationship with you (for example, for as long as you are employed with us

or receiving benefits from us);

- Whether there is a legal obligation to which we are subject (for example, certain laws require us to keep records of employment for a certain period of time after you are no longer employed with us);
- Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations); and/or
- Whether our operational needs require maintaining your personal information (for example, for the internal audit of bank operations, maintaining solicitation preferences – including for former and non-customers – systems administration, or for fraud prevention).

Procedure and Method for Destruction of Personal Information

The Company's procedure and method for destroying Personal Information is as follows:

- **Procedure:** Personal Information will be transferred to a separate storage drive (or separate document file for paper documents) and destroyed after retention for a certain period pursuant to the Company's internal policy or applicable laws and regulations (please refer to the provisions on retention and use period). Such Personal Information will not be used for any purpose other than the purpose permitted under the applicable laws and regulations.
- **Method:** Personal Information that has been printed on paper will be shredded through the use of document shredder or incinerated. Personal Information stored in electronic file form will be deleted by using technical means that will reasonably prevent data recovery.

6. Monitoring of Systems, Equipment and Property

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

Even if you create or have access to passwords to protect against unauthorized access to correspondence and activities, using that password does not make the related communications or activities private. In addition, phone calls, video calls, and/or instant messages or chats made or received on any business telephone or any Company device may be monitored or recorded for regulatory and compliance purposes. Monitoring may be conducted remotely or locally, and related Personal Information collected and processed by the Company, Affiliated Entities, and/or service providers to the Wells Fargo Group using software, hardware, or other means. Personal Information obtained through monitoring may be transferred to regulators and other authorities, Affiliated Entities and other recipients listed in [Section 3](#) as necessary for the Employment Purposes, including recipients in your country of residence or other jurisdictions.

Personal Information 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 Information that is used for monitoring, including appropriate training and supervision of responsible staff, and periodic review of monitoring programs. Personal Information obtained through monitoring, which is relevant to the purposes described above, will be retained for reasonable periods to accomplish these purposes, and subject to any rights employees may have under applicable law.

7. Exercising Rights Over Your Personal Information

You may have certain rights that enable you to have control and oversight over what organizations do with your Personal Information. If you are employed by us in South Korea, you may have the following rights under local data protection laws:

- Right to confirm whether your Personal Information is being processed.
- Right to be informed of processing activities relating to your Personal Information.
- Right to access and be provided with a copy of your Personal Information.
- Right to correct your Personal Information.
- Right to delete your Personal Information.
- Right to suspend the processing of your Personal Information.
- Right to refuse and request for explanations regarding fully automated decision-making using your Personal Information (if any).
- Right to consent, elect the scope of consent, and withdraw consent, to the processing of your Personal Information. 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 refuse or to accept a decision made through a fully automated processing of your Personal Information where it impacts your rights or obligations, and a right to request an explanation of such fully automated decision-making.
- Right to appropriate redress for any damage arising out of the processing of your Personal Information through a prompt and fair procedure.

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. Finally, you may also have the right to seek relief from the data protection authority in South Korea if you feel actions taken by us violate your privacy rights under South Korean laws and you are not satisfied with the resolution we provide. Details on how to contact the authority are available at its website [here](#).

If you have questions about or wish to exercise your Personal Information rights, please contact the APAC Regional Data Privacy Officer. The Company has also appointed a contact person ("**Contact Person**") to respond to your Personal Information Requests, questions, and complaints. The details of the APAC Regional Data Privacy Officer and Contact Person are found in [Section 8](#) below.

8. Contacting Us for Your Request

The Company has appointed the persons below to respond to requests in relation to your Personal Information.

APAC Regional Privacy Officer

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

Seoul Branch Contact Person and Privacy Officer

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

9. Consents

Please refer to the Employee Consent to Processing of Personal Information (including its Appendix) (the “**Consent**”) to voluntarily choose whether to consent to the collection, use, provision, transfer and other processing of your Personal Information (including sensitive information and unique identification information) as described in the Consent and this Notice.

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 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.