

WELLS FARGO NON-EMPLOYEE PRIVACY NOTICE

Korea

Effective: 1 November, 2015

"We" or "Company" refers to the Wells Fargo entity which has engaged the firm that employs you, or that you otherwise work for (the "Vendor"), to perform certain services for us. Under this engagement, you will be providing certain services to us on behalf of the Vendor, and we will act as the data controller regarding the collection, use, transfer, and processing of individually identifiable information about you ("**Personal Data**"). This document is referred to as the "**Notice**."

1. What Personal Data do we collect?

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

- **Master data:** first name and family name, date of birth, national tax and/or social insurance number;
- **Work contact details:** first name and family name, work address, work phone numbers, fax numbers, and work email address;
- **Emergency contact information:** first name and family name, and contact information (if provided by you) of a family member or nominated person to be contacted in an emergency;
- **Absence data:** dates of absence and reasons for absence (such as medical leave which may constitute sensitive personal data) to the extent these apply to you;
- **Performance data:** information pertaining to the quality and efficiency of the services you are rendering on behalf of the Vendor, against the agreed benchmarks between the Company and the Vendor and other similar assessment of performance;
- **Electronic usage data:** data about your use of equipment, electronic communications systems, and property, such as computers, mobile devices, email, internet, and voicemail; and
- **Disciplinary data:** information about conduct, investigations, and disciplinary matters, if any.

It is obligatory that you provide this information to the Company so that it can provide access to its systems and for the additional Engagement Purposes described below to the extent they apply to your engagement.

2. For what purposes do we use and process Personal Data?

The Company may use and process Personal Data to enable you to provide services to us under our engagement with the Vendor, including using and processing the following categories of Personal Data for the following purposes ("**Engagement Purposes**").

- **To provide performance metrics** to the Vendor (as your employer or agency), including assessment of the quality and quantity of the services provided under our agreement with the Vendor, the Company may process master data, work contact details, performance data, absence data, and disciplinary data.

- **To maintain and improve effective administration of our engagement with the Vendor**, including assigning projects and tasks, conducting resource analysis and planning, administering project costing and estimates, managing work activities, and administering compliance trainings, the Company may process work contact details, performance data, absence data, and disciplinary data.
- **To maintain a corporate directory**, including populating and making available contact details and/or an intranet website accessible by Company team members and authorized non-employees to facilitate communication with you, the Company may process work contact details and other data you voluntarily submit for these purposes.
- **To maintain information technology ("IT") systems**, including implementing and maintaining IT systems, providing IT support, ensuring business continuity, and managing security services and employee and non-employee access rights, the Company may process work contact details, electronic usage data, and disciplinary data.
- **To determine your suitability to be engaged**, at the time Vendor assigns you to provide services to Wells Fargo that require 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 Information 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 Information on such lists for purposes of future consultation, Company may process master data and disciplinary data.
- **To monitor and assure compliance with the Wells Fargo Code of Ethics and Business Conduct, other policies and procedures, and applicable laws**, including detecting or preventing possible loss or unauthorized access or processing of customer, confidential or restricted data, protecting Company and other party data and assets, conducting internal investigations, handling any potential or other claims, and engaging in disciplinary actions and terminations, the Company may process work contact details, absence data, performance data electronic usage data and disciplinary data.
- **To respond to requests and legal demands from regulators or other authorities**, including complying with requests from regulators or other authorities in your home country or other jurisdictions, and participating in legal investigations and proceedings including domestic and cross-border litigation and discovery procedures, such as attachment of earnings orders, and participating in legal proceedings including domestic and cross-border litigation and discovery procedures, the Company may process master data, work contact details, emergency contact information, performance data, electronic usage data, disciplinary data, and any other category of Personal Data necessary to respond to the request or legal demand.
- **To contact your family/partner of any emergencies**, the Company may process master data and emergency contact information.

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, such as to protect human life, safety or property, to improve public health or hygiene or promote the health of children, or to comply with domestic or international legal demands, or as authorized by you. For some activities, processing of certain Personal Data continues after individuals have left the service of the Company. However, the Company will endeavor not to keep Personal Data longer than necessary for the fulfillment of the

purposes outlined in this section, in accordance with our standard records retention periods, or as required or appropriate in the jurisdiction where such records or information is retained.

Procedure and Method for Destruction of Personal Data

In principle, the Company will promptly destroy the Personal Data in its possession once the Company achieves the purpose of collection and use of Personal Data. The process and means of destroying Personal Data are as follows.

Procedure: Personal Data will be transferred to a separate data base (or separate document file for paper documents) and destroyed after storage 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 Data will not be used for any purpose other than the purpose permitted under the applicable laws and regulations.

Method: Personal Data that has been printed on paper will be shredded through the use of document shredder or incinerated. Personal Data stored in electronic file form will be deleted by using technical means that will not allow data recovery.

3. Under what conditions is Personal Data transferred to other recipients?

The Company may transfer Personal Data to third parties for Engagement Purposes as described in Section 2 as follows:

- **Wells Fargo US.** 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 Wells Fargo Bank, N.A. operations in the US (collectively "**Wells Fargo US**"), the Company may transfer Personal Data to, or otherwise allow access to such data by, Wells Fargo & Company, 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 the Wells Fargo Code of Ethics and Business Conduct, other policies and procedures, and applicable laws; 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 managing your engagement 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 maintain a corporate directory; to maintain IT systems; to monitor and assure compliance with the Wells Fargo Code of Ethics and Business Conduct, other policies and procedures, and applicable laws; 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 list of the Affiliated Entities as of December 31, 2014 (see <http://www.sec.gov/Archives/edgar/data/72971/000007297115000449/wfc-12312014xex21.htm>).
- **Customers.** As necessary in connection with the Engagement Purposes, work contact details may be transferred to customers and other third parties.

- **Regulators, authorities, and certain third party controllers.** As necessary for the Engagement Purposes described above, Personal Data may be transferred to regulators, courts, and other authorities (e.g., tax and law enforcement authorities), and the Wells Fargo & Company Board of Directors.
- **Service providers.** As necessary for the Engagement 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, payroll, training, compliance, and other 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. 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 US, 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, 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 Engagement Purposes described above.

4. What security measures does the Company implement?

The Company will implement appropriate technical and organizational security measures to safeguard Personal Data. Recipients have been made aware that Personal Data may only be used in accordance with the purposes described in this Notice. When we retain a non-affiliated entity to perform a function, that entity will be required to protect workers' Personal Data.

Please bear in mind that if, as a result of your engagement you have access to Personal Information 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 Information and are prohibited from sharing such Personal Information with third parties, without authorization of the Company or the individuals. This obligation subsists even after the termination of your engagement.

5. How can I exercise access, correction, or other rights?

The Company has appointed a contact person ("**Contact Person**") to respond to your access and correction requests, questions and complaints.

Under applicable data protection laws, you may be entitled to request access to and/or correct, block or delete your Personal Data (including Sensitive Personal Data), or object to any use of Personal Data. If the Company will not be able to provide the requested information or make the change you request, you will be provided with reasons for the denial.

6. Under what circumstances are equipment, electronic communication systems, and property subject to monitoring?

To the extent permitted by local 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, text messaging, 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 and non-employee authorizations, as well as to monitor and assure compliance with the Wells Fargo 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. 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 made or received on any business telephone 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 & Company, 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, which is relevant to the purposes described above, will be retained for reasonable periods to accomplish these purposes, and subject to any rights team members may have under applicable law.

When carrying out monitoring use of our equipment or systems (including emails and phone calls) it will not normally be the Company's intention to access any Personal Data (except where it is relevant to the purposes described above), and we shall use our reasonable endeavors not to access, copy or use any Personal Data unless necessary. If such access occurs inadvertently, and it is not relevant to the purposes, we shall delete any and all such Personal Data as soon as it comes to our attention.

7. How do I reach the Contact Person for questions?

The Contact Person for the Company is:

APAC Data Privacy Officer
MAC Y1109-270
3 Pacific Place 1 Queens Rd East
27th Floor
Hong Kong, HKG
852 3650 8000
privacy.apac@wellsfargo.com

Please refer to the Consent to Collection, Use and Provision of Personal Data for Non-Employees to provide consents for processing of Personal Data as described in this notice.