WELLS FARGO
INTERNATIONAL NON-EMPLOYEE PRIVACY NOTICE

This Notice applies to the European Union (EU)

Effective: 1 May 2018

"**We,**" "**Our**" or "**Company**" refers to the Wells Fargo entity which has engaged the firm that employs you, or for which you otherwise work (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**."

Wells Fargo is one of the largest financial institutions in the world and operates globally. As described in Section 2 below, in order to manage your engagement, we need to collect, process, and use Personal Data. We also have to 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 EMEA Data Privacy Officer is listed in Section 7 below.

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 identification 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 of a family member or your nominated person to be contacted in an emergency (if provided by you).
- **Absence data:** dates of absence and reasons for absence (such as medical leave) 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 Wells Fargo equipment, electronic communications systems, and property, such as computers, mobile devices, email, internet, telephone and voicemail.
- **Disciplinary data:** information about conduct, disciplinary and grievance investigations, and disciplinary and grievance matters.

It is obligatory that you provide this information to the Company so that it can provide you with access to its systems and for the Engagement Purposes (described in Section 2) to the extent they apply to your engagement.

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

The Company uses and processes Personal Data for purposes of administering our contract with the Vendor, and for purposes of managing our business operations, including maintaining business continuity plans and processes, undertaking internal investigations and audits, handling legal claims, responding to requests from supervisory authorities, and complying with applicable laws and regulations on a global basis.

The Company also uses and processes 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 nonemployees 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 nonemployee access rights, the Company may process work contact details, computer usage data, and disciplinary data.
- **To determine your suitability to be engaged** at the time the 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 Data on the Wells Fargo and affiliates' "Do Not Hire" or "Do Not Reengage" lists, if Wells Fargo learns or determines, in its discretion, that you have committed a crime involving theft, fraud or dishonesty, or committed a 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.
- **To monitor and assure compliance with Wells Fargo's 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 courts, regulators or other authorities**, including complying with requests from courts, 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, the Company may process master data, work contact details, emergency contact information, absence data, performance data, electronic usage data, and disciplinary data.
- **To notify your family or emergency contacts in the event 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, or as authorized by you. For

some activities, processing of certain Personal Data continues after individuals cease providing services to 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. However, we may need to hold Personal Data beyond these time periods due to regulatory requirements of a particular country or in response to a regulatory audit, investigation or other legal matter. These requirements also apply to our third party service providers.

3. Under what conditions is Personal Data made available to recipients in different countries?

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

- **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 make Personal Data available 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 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 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 make Personal Data available 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 Wells Fargo's 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. See Exhibit 21 to the most recent Form 10-K we filed with the U.S. Securities and Exchange Commission at www.sec.gov/Archives/edgar/data/72971/000007297118000272/wfc-12312017xex21.htm for a select list of Affiliated Entities and subsidiaries as of December 31, 2017.
- **Customers and prospects.** As necessary in connection with the Engagement Purposes, work contact details may be transferred to customers and other third parties as permitted by applicable law.
- **Regulators, authorities, and other third parties.** 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), lawyers and consultants, independent external advisors (e.g., auditors), the Wells Fargo & Company Board of Directors, including to entities in the jurisdictions and other countries where Wells Fargo & Company and/or the Affiliated Entities are located.
- **Data processors.** 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, 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.

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, including executing agreements based on EU Model Contractual Clauses with respect to Personal Data transferred from the EU to a third country, 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. Please contact the EMEA Data Privacy Officer, using the contact information in Section 7, to obtain additional information about these safeguards.

4. What security measures does the Company implement?

Personal Data will be safely 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 our standards.

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 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 continues even after the termination of your engagement.

5. What are my rights in relation to Personal Data?

Laws in the EU enable you to have appropriate control and oversight over what organizations do with your Personal Data. This Notice provides you with details about your Personal Data rights. If you have questions about your Personal Data rights, or whether different local laws apply, please contact the EMEA Data Privacy Officer using the contact information in Section 7 below.

You have the following rights in relation to your Personal Data:

- **Access**: you can ask us for a description of the Personal Data we hold about you and our purposes for holding it; you can also ask for a paper or electronic copy of this information.
- **Rectification**: you can ask us to correct your Personal Data if you see that it is inaccurate or incomplete.
- **Objection**: you can object to our processing of your Personal Data where we base such processing on our legitimate interests or, when applicable, on public interests or where we act under an official authority.
- **Erasure**: you can ask us to destroy your Personal Data if you believe we no longer need it or we are inappropriately using it, or if you withdraw your consent. You can also ask for the destruction after you object to our use of your Personal Data or for compliance with a legal obligation.
- **Restriction of processing**: you can ask us to temporarily stop using your Personal Data when you contest its accuracy, when you believe our use is unlawful, or when you wish us to keep but not use your Personal Data beyond our time limit for storage for the purpose of a legal claim you've made or plan to make. You can also ask us to temporarily stop using your Personal Data during the period we are processing your objection request.
- **Data portability**: you have the right to receive Personal Data you have provided to us in a

structured, commonly used, and machine-readable format. You also have the right to request that we transmit your Personal Data directly to another party if technically feasible. This right only relates to Personal Data which we process based on your consent, or on a contract you have with us, and where we carry out the processing by automated means.

- **Complaint with a supervisory authority**: you have the right to lodge a complaint with a data protection supervisory authority.

In certain circumstances, we will need to use your Personal Data even though you may have asked us to delete it or restrict our use of it, or when you objected to our use. If this is necessary, we will do so in a lawful, fair, and transparent manner. Please contact the EMEA Data Privacy Officer listed in Section 7 below if you have any questions.

To the extent that consent is required by applicable law and our collection, use, disclosure or other processing of Personal Data is not otherwise permitted by applicable law, by providing Personal Data to the Company or to Wells Fargo & Company you consent to the collection, use, disclosure (including cross-border transfers to third countries), and other processing of Personal Data as described in this Notice. You may revoke consent at any time by notifying the EMEA Data Privacy Officer listed in Section 7 below. Prior uses and disclosures will not be affected (unless required by applicable law), and we may otherwise continue to process Personal Data as permitted or required by law. The consequences of revoking consent are explained in the last paragraph of Section 1 above.

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 access control authorizations, as well as to monitor and assure compliance with Wells Fargo's Code of Ethics and Business Conduct and other Company policies and procedures and disciplinary or grievance investigations. 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 legal, regulatory and compliance purposes and/or internal investigations. 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 Engagement Purposes described above, including recipients in your home country or other jurisdictions. Personal Data obtained through monitoring, which is relevant to the Engagement Purposes described above, will be retained for reasonable periods to accomplish these purposes, and subject to any rights nonemployees 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 absolutely 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 contact a Data Privacy Officer for questions?

The Company has regional Data Privacy Officers who are dedicated to responding to requests in relation to your Personal Data. Please contact the EMEA Data Privacy Officer using the contact information below:

EMEA Regional Data Privacy Officer
MAC Y1132-080
8th Floor, 1 Plantation Place
London, Great Britain
EC3M 3BD
Telephone: (44) 0-20-7149-8100
privacy.emea@wellsfargo.com