# Wells Fargo International Contingent Resource Privacy Notice

This Notice applies to the Bahamas, Japan, Mexico, Serbia, and the United Arab Emirates (DFIC).

**Effective:** 28 July 2022

"**We**," "**us,**" "**our**," or "**Wells Fargo**" 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 Wells Fargo 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 identification number or other personal 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 (if provided by you) of a family member or your nominated person to be contacted in an emergency;
- **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:** IP address, session identification information, any software you install on Wells Fargo equipment, and data about when and how you use and interact with Wells Fargo equipment, electronic communications systems, and property, through all applicable communication channels, computers, mobile devices, email, internet, intranet SharePoint sites, shared drives and other data repositories, including email, text, instant message or chat, transcriptions and/or telephone communications, voice recordings, video recordings, and presentations and virtual meetings hosted by Wells Fargo, and data about how your current use compares with benchmarks based on both your own prior use and others' use, and risk-rating scores based on such use.
- **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 access to its systems and for the additional Engagement Purposes described

below to the extent they apply to your engagement.

- **Public health data:** information relevant to public health, e.g., body temperature, symptoms, recent travel, potential or confirmed exposure, testing (including results) and vaccination status.

## 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 provide physical access to Wells Fargo offices/locations** and to issue physical access badges, the Company may process master data and work contact details.
- **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 employees 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 master data, 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 Data on the Wells Fargo and affiliates' "Do Not Hire" or "Do Not Reengage" lists, if Wells Fargo determines, in its discretion, that you have committed a crime involving theft, fraud or dishonesty or committed a serious violation of Wells Fargo's code of conduct or information security policies, and maintain the Personal Data on such lists for purposes of future consultation, Company may process master data and disciplinary data.
- **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, operating whistleblowing systems or channels, 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, and where permitted or required by law, disclose to third parties such as the police and/or other law enforcing authorities without consent, the Company may process master data, work contact details, emergency contact information, absence data, performance data, electronic usage data, and disciplinary data.

- **To contact your family/partner of any emergencies**, the Company may process master data and emergency contact information.
- **To comply with other employment-related legal requirements**, such as income tax, national insurance deductions, and applicable employment and immigration laws, the Company may process master data, work contact details, organizational data, visa and work permit data, contract data, and absence data.
- **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 public health data, which may include sensitive health 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. The Company will keep Personal Data no longer than necessary to fulfill the purposes outlined in this Notice. 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. The Company may need to hold Personal Data beyond retention periods in response to a regulatory audit, investigation or other legal matter. These requirements also apply to our third party service providers. Where required by law, Wells Fargo will anonymize data for additional processing.

## 3. Under what conditions is Personal Data made available to other recipients?

The Company may make the Personal Data described in Section 1 available to the following third parties for the Engagement Purposes described in Section 2:

- **Wells Fargo & Company.** 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**"), the Company may make Personal Data available 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 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 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 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 Wells Fargo & Company 10-K filing, Exhibit 21, made with the US Securities and Exchange Commission provides a list of select Affiliated Entities as of December 31, 2021(see https://www.sec.gov/Archives/edgar/data/72971/000007297122000096/wfc-1231x2021xex21.htm).

- **Customers and prospects.** As necessary in connection with the Engagement Purposes, work contact details may be transferred to customers and other third parties.
- **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 entities in the jurisdictions 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 will be subject to contractual obligations to implement appropriate administrative, technical, physical, and organizational security measures to safeguard Personal Data, and to process Personal Data only as instructed. Data Processors may carry out instructions related to IT system support, training, compliance, and other legitimate activities, and will be subject to contractual obligations to implement appropriate technical and organizational security measures to safeguard the Personal Data, and to process the Personal Data only as instructed.
- **Business transfers, combinations and related activities.** As we develop our business, the Wells Fargo Group might sell, buy, acquire, obtain, exchange, restructure or reorganize businesses or assets. In the event of any actual or proposed sale, merger, reorganization, transaction, restructuring, dissolution or any similar event involving our business or assets, Personal Data may be shared with the relevant entity or may be part of the transferred assets and will be subject to any necessary contractual obligations to ensure the protection of Personal Data.

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 & Company, 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. These measures enable us to transfer and use Personal Data 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.

To the extent that the sharing of Personal Data with the abovementioned third parties is subject to any Japanese data privacy laws, Wells Fargo is responsible for the management of Personal Data shared with such third parties, and the identity and contact details of Wells Fargo's representative is listed in Section 8 under the "Asia-Pacific" heading.

## 4. What security measures and record retention policies does the Company implement?

The Personal Data will be safely stored in the databases of the Company. The Company has implemented appropriate technical, physical and organizational security measures to safeguard Personal Data in accordance with security requirements of applicable law. Unfortunately, no data transmission or storage system can be guaranteed to be 100% secure. If you have reason to believe that your interaction with us is no longer secure, please immediately notify us in accordance with Section 10 below.

We will keep Personal Data no longer than necessary to: i) fulfill the purposes outlined in this Notice; ii) comply with legal or regulatory obligations to which Wells Fargo is subject; or iii) perform a contract duly established with you or in order to take steps at your request prior to entering a contract. We have implemented appropriate records retention policies to retain Personal Data only to the extent permitted by applicable laws. We may need to hold Personal Data beyond retention

periods in response to a regulatory audit, investigation, or other legal matter. These requirements also apply to our third party service providers. Where required by law, Wells Fargo will anonymize data for additional processing.

Please bear in mind that if, as a result of your engagement you have access to Personal Data of the Company or any of its controlling, subsidiary or affiliated entities, its clients and/or service providers or any third parties, you are obliged to maintain the confidentiality of such Personal Data and are prohibited from sharing such Personal Data with third parties, without authorization of the Company or the individuals. This obligation subsists even after the termination of your engagement.

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

- You may have certain rights under applicable local law to know, update and amend your Personal Data and other rights under local law. These rights may include the right to seek relief from data protection authorities and the right to request access, correction, deletion and suspension of use, to restrict or object to processing, and the right to data portability of your Personal Data. In addition, to the extent required by applicable law, an overview of entities involved in the processing of your Personal Data, including the identity of certain recipients of your Personal Data and/or the countries where your Personal Data is being processed, may be made available upon request. The abovementioned rights may not be absolute, and exceptions may be applicable. If Wells Fargo is not able to accommodate your request, you will be provided with the reasons for the denial. If you have questions about your Personal Data rights, or whether different local laws apply, please contact the applicable Regional Data Privacy Officer using the contact information in Section 8 below.
- You may have a right under applicable law to make a complaint about this Notice. If you would like to make a complaint, please submit your complaint in writing using the contact details below most applicable to your location. We will respond to a written complaint within 30 days or within such other period as required by applicable law. If you are not satisfied with our response, you may be able to pursue your complaint with your data protection authority or the privacy commissioner for your country.

The Company has appointed a contact person ("**Contact Person**") to respond to your access and correction requests, questions and complaints. The Contact Person is generally the Human Resources Manager at the Company or, if there is no Human Resources Manager, the Branch Manager or Country Manager for that location.

## 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, security door access records, computer use activity, voice recordings, video recordings, and presentations hosted by Wells Fargo 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, investigate, and assure compliance with the Wells Fargo Code of Ethics and Business Conduct and other Company policies and procedures and disciplinary or grievance investigations. The Company also monitors so to ensure the security of its facilities. 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.

The Company 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.

## 7. What about changes to this Notice?

This Notice may be modified as a result of amendments to the law or regulations or due to other reasons. In such case, an amended Notice will be posted on our website at http://www.wellsfargo.com/privacy_security/. The page providing the Notice shall contain a date as to when the Notice was last updated.

## 8. How do I contact a Regional Privacy Officer for questions?

The Company has appointed Regional Privacy Officers (as listed below) who are responsible for responding to requests in relation to your Personal Data.

**Canada, Latin America and Caribbean:**
Americas Regional Privacy Officer
23rd Floor, 22 Adelaide Street West
Toronto, Ontario
Canada M5H-4E3
Telephone: (416) 607-2900
canadaprivacyinfo@wellsfargo.com
privacy.latinamerica@wellsfargo.com

**Europe, Middle East and Africa**
EMEA Regional Privacy Officer
33 King William Street
London, United Kingdom
EC4R 9AT
Telephone: +44(0) (203) 942-8000
privacy.emea@wellsfargo.com

**Asia-Pacific:**
APAC Regional Privacy Officer
138 Market St
#30-01 CapitaGreen
Singapore, 048946
Telephone: (65) 6395 6900
privacy.apac@wellsfargo.com

**Acknowledgement and Consent**

I understand that Wells Fargo will collect, use, transfer and disclose the Personal Data about me as described in this Notice. By signing below or clicking the accept button, if acknowledged electronically, I confirm my consent to the collection, processing, use, transfer and disclosure of my Personal Data for the purposes and on the terms set out above and agree that this Notice and Consent supersedes any prior notice on this subject and shall cover all Personal Data collected or maintained by Wells Fargo in connection with my engagement to perform services for Wells Fargo.

| | |
|---|---|
| Legal Name (Printed) | Taxpayer ID/SSN |
| Signature | Date |