
Europe, Middle East and Africa (EMEA)

Wells Fargo International Employee Privacy Notice

This notice applies to the United Kingdom (“**UK**”), countries in the European Union (“**EU**”) and the Dubai International Financial Center (“**DIFC**”) (collectively, “**EMEA**”).

Effective: 25 June 2025

In this document, the terms "we," "our," "us," or "Company" refer to the Wells Fargo entity listed in Section 12 with which you have an employment contract and which is acting as the data controller for the processing of information related to you ("**Personal Data**"). The terms "you" or "your" refers to an individual who has an employment contract or employment relationship with the Company. This document is referred to as the "Notice."

Wells Fargo is one of the largest financial institutions in the world and operates globally. As described in Section 3, in order to carry out employment-related operations, including administering your contract or employment relationship with the Company, we need to process certain Personal Data, as described below.

Name of group parent: Wells Fargo & Company

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

Contact information for our EMEA Regional Privacy Officer is listed in Section 11. “Wells Fargo” means Wells Fargo & Company and its affiliates and subsidiaries.

1. What Personal Data do we collect?

We may collect the following categories of Personal Data in connection with your employment and to the extent permitted under applicable law:

- **General data:** first name, middle name, and surname (including any previous names used); personal contact details (home and mobile telephone numbers, email addresses, and home address); date and place of birth; citizenship; marital status; gender; data on your background and schooling to understand your social mobility; and veteran/military status.
- **Position or employment/work description:** employer; title; position held; length of tenure and work authorization status.
- **Identification and Authentication data:** national or governmental identification such as passport or national identification card; driver's license; national insurance number or tax and/or social insurance number; information required for tax reporting; health insurance information; home address and telephone number; documents that verify address; date of birth; country of domicile; documents that verify employment; and signature authorization or information we use to identify and authenticate you e.g. your signature or additional information we get from external sources that we need for compliance purposes.
- **Financial data and payment details:** salary and other income; bank account details and financial relationships.
- **Background or credit check data:** to the extent required or permitted by local law, credit check information and background check information including credit and criminal checks and screening; prior employment

history; current and past directorships held by you or by members of your immediate family; data associated with verification of politically exposed persons; education history; professional memberships and qualifications; professional or personal references; and other information contained in your curriculum vitae or resume.

- **Qualifications data:** information concerning any qualifications you hold e.g. university education, professional certifications.
- **Visa and work permit data:** copies of your passport; birth certificate; national identification card; existing and expired visa(s) and other permit details; and all such information about relevant members of your family (such as your parents, spouse, domestic/civil partner, children and/or other dependents), if required by law.
- **Emergency contact information:** first name and last name and contact information of a family member to be contacted in an emergency.
- **Work contact details:** work address; work phone numbers; fax numbers; and work email address.
- **Contract data:** terms and conditions of your contract; salary or pay; other contractual benefits such as car, educational or housing allowances; stock, incentive or bonus awards; details of applicable bonuses, incentives, and commission plans; and changes to the terms and conditions of your employment or work relationship.
- **Organizational data:** title; job position; function; employee ID; department; business unit; supervisor's name and higher-level supervisor(s); cost center; signing authority; skills; work experience at the Company; user ID; information technology access rights (such as user and system IDs and passwords); and electronic content you produce using company systems.
- **Employment data:** data that may be collected in the course of employment including business travel; business expenses; use of Company facilities; training activity; and attendance at the office and Company events.
- **Access or system usage data:** information given by completing forms and surveys as well as data about your use of our systems, including authentication credentials such as usernames or IDs and passwords to log into portals; location data; user display name and identifier; other website or product access information.
- **Computer usage data:** data about your use of (for instance, how, when and where you use and interact with) equipment, electronic communications systems, and property, such as computers, mobile devices, email, instant message, internet, intranet SharePoint sites, shared drives and other data repositories, and voicemail.
- **Market data:** information from market research, any data obtained, and opinions expressed when participating in any surveys.
- **Geographical data:** information about your location e.g. about any working location monitoring for transfer pricing or other compliance purposes.
- **Performance data:** performance evaluations; appraisals; promotions and assessments of performance; development programs planned and attended; e-learning programs; willingness to relocate; information used to populate employee biographies; and licence/registration data.
- **Disciplinary data:** information about conduct, investigations, and disciplinary notices, if any.
- **Absence data:** dates of absence and reasons for absence (such as medical leave) to the extent that these apply to you.
- **Investigation data:** data collected for Wells Fargo investigation process (if used) e.g. due diligence checks, fraud, sanctions and anti-money laundering checks, external intelligence reports, and content and metadata related to relevant exchanges of information among individuals, organizations, including, emails, live chat, video calls, voicemail etc.
- **Complaints data:** data collected for the processing in relation to any Wells Fargo complaints procedures.
- **Regulatory data:** information we need to support our regulatory obligations.

- **Benefits information:** car, mobile device, and housing allowance; contribution to health insurance; pension contribution; and the name, address, and date of birth of your spouse or domestic/civil partner and/or dependents who are your beneficiaries.
- **Third-party data:** the name, title, employer, contact details, and location of any individual whom you are related to or have a close personal relationship with, and who: (i) provided you with a reference for employment with the Company; (ii) is a U.S. or non-U.S. government official; or (iii) has decision-making authority/capability over any matters affecting the Company.
- **Cookies and similar technologies:** data that websites store and access on your computer or mobile device when you visit a website, allowing a website to recognize your visit and collect information about how you use that website. The Company uses these technologies to recognize you, remember your preferences and tailor the content we provide to you.
- **Sensitive Personal Data:** The Company may also collect certain types of Sensitive Personal Data as permitted and/or required by local law or with your explicit consent, such as health or medical information (e.g. health and sickness records and long-term health conditions), disability status, gender identity, pronouns, sexual orientation, biometric data, trade union membership information, religious beliefs and faiths, and data related to race or ethnicity (collectively, "**Sensitive Personal Data**"). We collect this information for specific purposes, such as health/medical information in order to accommodate a disability or illness and to provide benefits (including any flexible working from home benefits); religion or church affiliation in countries such as Germany where required for statutory tax deductions; and diversity-related Personal Data (such as race or ethnicity) in order to comply with legal obligations and internal policies relating to diversity and anti-discrimination. As explained in Section 3, we will only use such sensitive information for those purposes and as permitted by law.

2. What are the obligations of employees in this context?

If you provide the Company with Personal Data about your spouse or domestic/civil partner, your respective children, other dependents or other third parties, it is your responsibility to inform them: (i) of their rights with respect to such Personal Data; and (ii) that you may disclose their Personal Data to the Company and for which purposes. You are also responsible for obtaining consent from these individuals (unless you are authorized to give such consent on their behalf) if such consent is required by law for the processing of their Personal Data.

You further agree to follow applicable law and the Company's policies, standards and procedures brought to your attention when handling any Personal Data to which you have access in the course of your relationship with the Company. In particular, you will not process any Personal Data for any purpose other than in connection with and to the extent necessary for your work in the Company. You understand that these obligations continue to exist after the termination of your relationship with the Company.

3. For what purposes do we use Personal Data and under which lawful bases?

The Company uses Personal Data for the purposes listed below based on one or more of the following lawful bases:

- because we are required to do so by local law;
- because such information is necessary to fulfill the employment contract;
- because this information is necessary to protect the vital interests of any person;
- because this information is necessary for the performance of a task carried out in the public interest (e.g. for the purpose of preventing or detecting crime or fraud); because you voluntarily provide this information and give your consent for us to process it;
- because we have a specific legitimate interest to process it. In such cases, we have a legitimate interest in processing Personal Data, for example, (i) to ensure that our networks and information are secure; and (ii) to administer and generally conduct business within the Company and across the organization;
- to comply with a legal obligation;

- to establish, utilize and defend our legal rights;
- for insurance purposes;
- For the UK only, we also use Sensitive Personal Data for the purposes of monitoring equality of opportunity or treatment generally amongst our staff including with the appointment of senior employees within the business and to track social mobility amongst our workforce. This is considered to be a use of data for our legitimate interests and/or substantial public interests under UK law.

The Company processes the following categories of Personal Data for the following purposes ("**Employment Purposes**"), as permitted by applicable law.

- **Providing compensation**, including payroll, bonus, stock options, and incentives, as applicable.
 - For this purpose, the Company may process general data, position or employment/work description, identification and authentication data, access or system usage data, organizational data, work contact, financial data and payment details, contract data, employment data, performance data, absence data, and benefits information.
 - We process such data because such data is necessary to carry out an agreement we have with you; because we have a specific legitimate interest to process it; or to comply with a legal obligation.
- **Providing rights, benefits (e.g. health care or pensions or working from home), entitlements**, and other conditions, as applicable.
 - For this purpose, the Company may process general data, position or employment/work description, work contact details, organizational data, contract data, performance data, geographical data, absence data, benefits information, Sensitive Personal Data, employment data, and visa and work permit data.
 - We process such data because such data is necessary to carry out an agreement we have with you; because we have a specific legitimate interest to process it; to comply with a legal obligation; or, where applicable, you voluntarily provide this information and give your consent for us to process it.
- **Complying with other employment-related legal requirements**, such as income tax, national insurance deductions, and employment and immigration laws.
 - For this purpose, the Company may process general data, position or employment/work description, organizational data, identification and authentication data, access or system usage data, work contact data, financial data and payment details, contract data, employment data, performance data, absence data, geographical data, qualifications data, third-party data, visa and work permit data.
 - We process such data because such data is necessary to carry out an agreement we have with you; because we have a specific legitimate interest to process it to comply with a legal obligation; to establish, utilize and defend our legal rights; or, where applicable, you voluntarily provide this information and give your consent for us to process it.
- **Maintaining and improving effective administration of the workforce and Company facilities**, including: assigning projects and tasks; making business travel arrangements; managing business expenses and reimbursements; managing and administering vacation time, office time, and (sickness) absence leave; conducting workforce analysis and planning; administering project costing and estimates; managing work activities; managing secondments and transfers; providing performance evaluations and promotions; conducting talent management; succession planning and career development; 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); and providing facilities management and worksite security.
 - For this purpose, the Company may process general data, position or employment/work description, organizational data, identification and authentication data, access or system usage data, background or credit check data, visa and work permit data, financial data and payment details, work contact details, emergency contact information, contract data, performance data, absence data, employment data,

geographical data, qualifications data, third-party data, market data, complaints data, regulatory data, investigation data, disciplinary data, benefits information as well as Sensitive Personal Data.

- We process such data because such data is necessary to carry out an agreement we have with you; because we have a specific legitimate interest to process it; to comply with a legal obligation; to establish, utilize and defend our legal rights; or, where applicable, you voluntarily provide this information and give your consent for us to process it.
- **Managing business operations and for contractual and litigation-related purposes**, including initiating or defending claims, performance and service of contracts, including maintaining records relating to business activities, budgeting, financial management and reporting, business continuity, communications, managing mergers, acquisitions, sales, re-organizations or disposals, and integration with a purchaser.
 - For this purpose, the Company may process general data, position or employment/work description, work contact details, organizational data, contract data, employment data, benefits information, third-party data, access or system usage data, computer usage data (including devising and implementing methodologies such as risk ratings), geographical data, complaints data, regulatory data, investigation data and disciplinary data and all other relevant data.
 - We process such data because such data is necessary to carry out an agreement we have with you; because we have a specific legitimate interest to process it; to comply with a legal obligation; or to establish, utilize and defend our legal rights.
- **Maintaining a corporate directory and allow for staff communications**, including populating and making available contact details and/or an intranet website (accessible by Company employees and authorized contingent resources) to facilitate communication with you or the sharing of information internally.
 - For this purpose, the Company may process general data, work contact details, position or employment/work description, organizational data and other data you voluntarily submit such as photographs.
 - We process such data because we have a specific legitimate interest to process it.
- **Managing and maintaining information technology ("IT") systems, and for any analytical purposes**, including implementing, maintaining, and operating IT and communication systems; providing IT support and asset management; maintaining business continuity and crisis management plans and processes; managing security services and employee access rights; compiling of audit trails and other reporting tools; identifying patterns, establishing and implementing risk rating tools in the use of technology systems and information entrusted to us to protect Company people, assets and property as well as to comply with any regulatory requirements or demands.
 - For this purpose, the Company may process general data, position or employment/work description, work contact details, organizational data, contract data, employment data, access or system usage data, computer usage data (including devising and implementing methodologies such as risk ratings as well as analyzing or collating platform traffic or content views), geographical data, complaints data, regulatory data, investigation data, disciplinary data and all other relevant data types.
 - We process such data because we have a specific legitimate interest to process it; or, for the performance of a contract (for e.g. enforcement of our terms and conditions of use); or, to comply with a legal obligation; or, where required under applicable local laws, you give your consent for us to process the data (for e.g. where you have consented via the relevant website).
- **Monitoring, investigating and assuring compliance with Wells Fargo's Code of Ethics and Business Conduct, other policies and procedures, and applicable laws**, including Company policies and procedures with regard to monitoring and recording of telephone calls, voicemail instant messaging, original and back-up copies of email, video (including CCTV), Internet and other Company resources, and other monitoring activities as permitted by local law; complying with legal and other requirements applicable to our businesses in all countries in which we operate, such as record-keeping and reporting obligations; conducting audits; conducting background checks detecting or preventing possible loss or unauthorized access or processing of

customer, employee, confidential or restricted data; protecting Company and other party data and assets, conducting internal investigations, including employee reporting of allegations of wrongdoing policy violations, fraud, or financial reporting concerns; and complying with internal policies and procedures; handling any potential or other claims; and engaging in disciplinary actions, grievances, and terminations.

- For this purpose, the Company may process general data, position or employment/work description, work contact details, organizational data, contract data, employment data, access or system usage data, computer usage data (including devising and implementing methodologies such as risk ratings), geographical data, absence data, identification and authentication data, background or credit check data, third-party data, Sensitive Personal Data, performance data, complaints data, regulatory data, investigation data, disciplinary data and all other relevant data as needed.
- We process such data because we have a specific legitimate interest to process it; or, for the performance of a contract; or, to comply with a legal obligation; or to establish, utilize and defend our legal rights; or, where required under applicable local laws, you give your consent for us to process the data.
- **Responding to requests and legal demands from courts, regulators or other authorities**, including complying with inspections and other requests from regulators or other authorities in your home country or other jurisdictions, such as attachment of earnings orders, and participating in and responding to legal process including domestic and cross-border litigation, subpoenas pursuing legal rights and remedies, defending litigation, and managing any internal complaints or claims and discovery procedures (including legal proceedings which may occur outside your jurisdiction of residence).
 - For this purpose, the Company may process general data, position or employment/work description, work contact details, organizational data, contract data, employment data, access or system usage data, computer usage data (including devising and implementing methodologies such as risk ratings), geographical data, absence data, identification and authentication data, background or credit check data, third-party data, Sensitive Personal Data, performance data, complaints data, regulatory data, investigation data, disciplinary data and all other relevant data as needed.
 - We process such data because such data is necessary to carry out an agreement we have with you; because we have a specific legitimate interest to process it; to comply with a legal obligation; or to establish, utilize and defend our legal rights.
- **Responding to emergencies, including contacting you or your family or emergency contacts in the event of any emergencies**, protecting the health and security/safety of employees and others, and protecting office equipment, facilities, assets and other property.
 - For this purpose, the Company may process general data, work contact details, emergency contact information, organizational data and other data you voluntarily submit.
 - We process such data because we have a specific legitimate interest to process it.
- **Managing and maintaining programs applicable to remote access, bring your own device or mobility**, including ensuring compliance of any privately-owned equipment (e.g., mobile phones, laptops, tablets, and similar/hybrid devices) with and to the extent these are subject to policies applicable to remote access, bring your own device (“BYOD”) or mobility or the Corporate Participant Agreement (where applicable) (https://now.wf.com/sp?id=kb_article&sysparm_article=KB0078286&sys_kb_id=cb27c1e747a58ad8bbfef6da516d436b&spa=1) and other relevant internal policies (such as those related to monitoring, as outlined below), as applicable to you. Review these policies for additional details about the program. Processing subject to these policies includes the overall management of the program and lifecycle of applicable devices; verification of your compliance with applicable policies; maintenance of applicable systems/on-device infrastructure; reimbursement management, if applicable; providing remote and in-person (where necessary) maintenance, support and security intervention; verification of device compatibility and security requirements in line with applicable internal policies (e.g., using mobile device management solutions to verify access to Company networks/systems through the applicable device); location verification (e.g.,

country check for security purposes); and other processing required for compliance with any additional regulatory requirements.

- For this purpose, the Company may process general data, position or employment/work description, identification and authentication data, financial data and payment details, work contact details, contract data, organizational data, employment data, access or system usage data, computer usage data, geographical data, investigation data, complaints data, regulatory data, and all other relevant data as needed.
- We process such data because we have a specific legitimate interest to process it; or, where required under applicable local laws, you give your consent for us to process the data.
- **Performing certain limited activities with respect to Sensitive Personal Data**, as required or permitted under local law, such as calculating the number of sick days for statutory wage tracking, assessing benefits (including any flexible working from home benefits), reporting workplace accidents, complying with obligations to make reasonable adjustments and with other disability discrimination legislation, as well as our pay and conditions, confirming someone's right to work, and verifying identity for security purposes.
 - For this purpose, the Company may process general data, market data and Sensitive Personal Data.
 - We process such data in order to comply with a legal obligation; or, where applicable, you voluntarily provide this information and give your consent for us to process it.
- **Carrying out diversity monitoring which usually includes Sensitive Personal Data**, as permitted by local law or with your explicit consent. This includes monitoring equal opportunities such as reviewing our interviewing and hiring processes, running reports to understand seniority of staff, our existing staff population and promotions. Additionally, we may collect this data to report on diversity in compensation and to identify suitable existing employees to be promoted.
 - For this purpose, the Company may process general data, position or employment/ work description data, financial data, organization data and Sensitive Personal Data.
 - We process such Sensitive Personal Data usually on the basis of your explicit consent unless local law permits us to collect and use this data for this purpose. Please note that when we obtain your consent to use your Sensitive Personal Data you can choose not to provide your consent. You will not experience any detriment should you choose not to consent. We otherwise rely on our legitimate interests to process this data for this purpose since we wish to understand the diversity of our workforce and promote a more diverse workforce.

4. To whom do we disclose Personal Data?

Wells Fargo operates across the globe, and we may transfer Personal Data for Employment Purposes to Wells Fargo entities located outside of the UK, the EU and/or DIFC. Cross-border transfers can also occur when we engage third parties to assist us with certain operations and activities if established in different countries, including countries located outside of the UK, the EU and DIFC.

The countries where we have operations are shown on this map at <https://www.wellsfargo.com/cib/global-services/locations/>. We may also transfer Personal Data to other countries where our third-party service providers are located.

Disclosure of and access to Personal Data within the Company will be limited to those who need to know the information for Employment Purposes and will include your managers and their designees, and personnel in HR, IT, Compliance, Legal, Finance and Accounting, and in Internal Audit. All personnel within the Company will generally have access to your business contact information such as name, position, telephone number, postal address, and email address.

The Company may transfer Personal Data for Employment Purposes to the following recipients:

- **Wells Fargo U.S.** Since management, human resources, legal, and audit responsibility partially rests with Wells Fargo & Company as the group parent in the United States ("**Wells Fargo & Company**") and with Wells Fargo Bank, N.A. operations in the U.S. ("**Wells Fargo Bank, N.A.**") (collectively, "**Wells Fargo U.S.**"), the Company may transfer Personal Data to, or otherwise allow access to such data by, Wells Fargo U.S., which may process

Personal Data for the following purposes: maintaining and improving effective administration of the workforce; providing rights, benefits, stock grants, and entitlements; maintaining a corporate directory; maintaining IT systems; monitoring, investigating and assuring compliance with Wells Fargo's Code of Ethics and Business Conduct, other policies and procedures, and applicable laws; managing and maintaining the applicable programs in relation to remote access, BYOD and mobility; and responding to requests and legal demands from regulators and other authorities, including such authorities in the United States. In certain circumstances, Wells Fargo & Company or Wells Fargo Bank, N.A. may act as an independent controller of your Personal Data. If you have any questions, please contact our EMEA Regional Privacy Officer, using the contact information in Section 11.

- **Affiliated Entities.** To the extent that your management or the human resources responsibility for overseeing your employment relationship with the Company partially rests with different Wells Fargo entities ("**Affiliated Entities**"), the Company may also transfer Personal Data to, or otherwise allow access to such data by, relevant Affiliated Entities, which may process Personal Data for the following purposes:
 - maintaining and improving effective administration of the workforce; providing rights, benefits, stock grants, and entitlements; maintaining a corporate directory; maintaining IT systems; monitoring, investigating and assuring compliance with Wells Fargo's Code of Ethics and Business Conduct, other policies and procedures, and applicable laws; managing and maintaining the applicable programs in relation to remote access, BYOD and mobility; and
 - responding to requests and legal demands from regulators and other authorities, including authorities in the jurisdictions where our Affiliated Entities are located. If you have any questions, please contact our EMEA Regional Privacy Officer, using the contact information in Section 11.
- **Customers and Prospects.** As necessary and in connection with business operations, Personal Data may be transferred to customers and other third parties as permitted by applicable law. In certain limited circumstances, general data, visa and work permit data, and organizational data may also be transferred to third parties, for example, if required by the third party to comply with its legal obligations, such as carrying out their due diligence and know-your-customer checks.
- **Regulators and other Public and Governmental Authorities.** As necessary and in connection with the Employment Purposes as described in Section 3, Personal Data may be transferred to regulators, courts, and other authorities (e.g., tax and law enforcement authorities).
- **Acquiring Entities.** If the Wells Fargo entity for which you work is (or is contemplated to be) sold or transferred in whole or in part, your Personal Data may be transferred to the new employer or potential new employer, including to the jurisdictions and other countries where these entities are located, subject to any rights provided by applicable law.
- **Service Providers.** As necessary and in connection with the Employment Purposes as described in Section 3, 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, monitoring 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 permitted by the contract. In addition, to the extent that Personal Data are disclosed to independent external auditors, benefits providers, insurance carriers, or other service providers that may not be acting solely as a Data Processor, such service providers will be subject to any necessary contractual obligations regarding the protection and processing of such information.
- **Professional Advisors.** This category includes accountants, auditors, lawyers, insurers, bankers, and other outside professional advisors in all of the countries where we operate. As necessary and in connection with the Employment Purposes as described in Section 3, Personal Data may be shared with one or more professional advisors.

Transferring your data cross-border: We may need to transfer your information in this way for a variety of purposes such as to carry out our contract with you, to fulfil our legal obligation, to protect the public interest, and/or for our

legitimate interests. The recipients of Personal Data identified in this Section 4 may be located in the United States and other jurisdictions. Some of these countries are recognized by the EU or the UK or the DIFC respectively as providing an adequate level of protection according to each of their respective standards (for instance, the full list of these countries recognized under EU law is available at https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en). With regard to transfers from the EU, the UK or the DIFC to countries not considered adequate by the relevant Data Protection Authority, we have put in place safeguards and adequate measures to protect Personal Data, such as standard contractual clauses as adopted by the EU, the UK or the DIFC respectively. Please contact our EMEA Regional Privacy Officer, using the contact information in Section 11, to obtain a copy of these safeguards and measures.

5. From which other sources do we receive Personal Data?

In addition to Personal Data that we receive directly or indirectly from you, we may receive your Personal Data from certain other sources. These may include:

- Colleagues;
- Managers;
- Prior employers or schools;
- Clients;
- Government databases;
- Credit reference agencies;
- Criminal records agencies; and
- Background screening vendors.

We may conduct enhanced background checks for specific high-risk roles within Wells Fargo and these roles will be identified as such. This will be carried out during recruitment and periodically throughout your employment, in line with Wells Fargo policies and procedures.

6. How long do we retain Personal Data?

We retain Personal Data for as long as needed or permitted in light of the purpose(s) for which the data were obtained and consistent with applicable law. The criteria used to determine our retention periods include but are not limited to:

- 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); and/or
- 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); and/or
- 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 data (for example, for the internal audit of bank operations, maintaining solicitation preferences (including for former customers and non-customers), systems administration, or for fraud prevention; and/or
- 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); and/or
- 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 data (for example, for the internal audit of bank operations, maintaining solicitation preferences (including for former customers and non-customers), systems administration, or for fraud prevention).

7. What security measures do we implement?

The Company has implemented appropriate technical, physical and organizational security measures to safeguard Personal Data in accordance with the Wells Fargo Information Security Policy and standards. When we retain a non-Affiliated Entity or Data Processor to perform a function, that entity will be required to protect your Personal Data in accordance with our standards. 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 11.

8. What are your rights in relation to Personal Data?

What are your rights?

You have the right to request to access, rectify, erase, or restrict processing of Personal Data, or request to receive a copy of your Personal Data for purposes of transmitting it to another company (to the extent these rights are provided to you by applicable law). To exercise these rights, or submit a complaint in relation to these rights, contact our EMEA Regional Privacy Officer using the information in Section 11. We will respond to your request consistent with applicable law.

How can you revoke consent to our processing of your Personal Data?

To the extent that consent is required by applicable law, we will seek your consent.

You may revoke your consent at any time by notifying the EMEA Regional Privacy Officer using the contact details in Section 11. Prior uses and disclosures of Personal Data, however, will not be affected by the withdrawal of consent (unless required by applicable law), and we may continue to process Personal Data as permitted or required by law.

How can you object to automated decision-making and/or profiling?

You may object to the use of your personal data for the purposes of automated decision-making and/or profiling, by contacting the EMEA Regional Privacy Officer using the contact information in Section 11. We may use automated methods of processing such as Artificial Intelligence systems or models (“AI”) to optimize and increase the efficiency of business processes and/or to support and enhance security controls. By using AI, we do not intend to make automated decisions about you and therefore its application would not produce any legal or equivalent effects concerning you unless stated otherwise in a specific notice provided to you directly.

In addition to our EMEA Regional Privacy Officer listed in Section 11, the Company has appointed a person to respond to your questions and complaints (“**Contact Person**”). 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.

You also may lodge a complaint with a Data Protection Authority for your country or region or in the place of the alleged misconduct. Contact information for the relevant Data Protection Authority may be found by clicking on link(s) below:

United Kingdom	Information Commissioner's Office (ICO)
European Union	Our Members European Data Protection Board (europa.eu)
DIFC	Data Protection DIFC

9. Under what circumstances are equipment, electronic communications systems and property subject to monitoring?

To the extent permitted by local law and regulations, and subject to any other local notices or policies, the Company reserves the right to monitor and/or record 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, telephone calls and CCTV. For more information, please visit the Global Employee Handbook (https://hop.wellsfargo.com/ent_bb_0005), the Code of Ethics and Business Conduct (https://hop.wf.com/ethics_ee_bestbet02), Wells Fargo’s Information Security Policy

(https://hop.wellsfargo.com/ent_bb_0005), and other policies applicable to remote access, BYOD or mobility or the Corporate Participant Agreement (<https://hop.wf.com/4j7t>), as applicable to you.

In addition, subject to any other local notices or policies (including those referenced above), the Company may engage in such activities to administer IT access, provide IT support, manage security services and employee authorizations, as well as to monitor, investigate and assure compliance with Wells Fargo's Code of Ethics and Business Conduct, and other Company policies and procedures. As consistent with applicable law, 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 applicable policies in relation to remote access, BYOD or mobility, as referenced above, which you should review if you use an approved device. 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, to the extent permitted by local law, 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 U.S., Affiliated Entities, and/or Data Processors using software, hardware or other means. Personal Data obtained through monitoring may be transferred to regulators and other authorities, as well as the Wells Fargo & Company Board of Directors, and other recipients as necessary for the purposes described above, including recipients in your home country or other jurisdictions. Personal Data obtained through monitoring will be safeguarded in accordance with the security measures set out in Section 7. Personal Data obtained through monitoring, which is relevant to the purposes described above, will be retained for the time periods described in Section 6 subject to any rights employees may have under applicable law.

When carrying out monitoring of use of our equipment or systems, the Company implements appropriate measures to protect against abuse of use of any such Personal Data that is processed in connection with such monitoring such as training and supervision of staff and periodic review of procedures and programs.

Our websites, apps and other digital products may also track and record your interactions with them to help:

- Provide or improve services and features;
- Keep you safe;
- Keep our services secure;
- Make your visit more personal; or
- Support our marketing.

Some tracking is essential but other tracking is optional.

For more details, please refer to: <https://www.wellsfargo.com/privacy-security/>.

10. How do we update 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.

11. Who do you contact for questions on your Personal Data?

The relevant Wells Fargo entity or Company has Regional Privacy Officer(s) who are dedicated to responding to requests in relation to your Personal Data. For the Wells Fargo entities listed in Section 12, please contact our EMEA Regional Privacy Officer using the contact information below:

EMEA Regional Privacy Officer
Address: 33 King William Street, London, United Kingdom, EC4R 9AT

Telephone: +44 (0) 203-942-8000
Email: privacy.emea@wellsfargo.com

12. What Wells Fargo entities operate in EMEA?

You have an employment relationship with one of the Wells Fargo legal entities set out in your contract of employment. A list of entities that Wells Fargo operates in EMEA can be found below:

Name of Wells Fargo Legal Entity	Jurisdiction
Wells Fargo Bank, National Association, London Branch	United Kingdom
Wells Fargo Securities International Limited	United Kingdom
Wells Capital Finance (UK) Limited	United Kingdom
Wells Fargo Bank International Unlimited Company	Ireland
Wells Fargo Bank International Unlimited Company, Frankfurt Branch	Germany
Wells Fargo Bank International Unlimited Company, Frankfurt Branch, the Dusseldorf Office	Germany
Wells Fargo International Finance (France) S.A.S.	France
Wells Fargo Securities Europe S.A.	France
Wells Fargo Capital Finance (UK) Limited, Amsterdam Branch	The Netherlands
Wells Fargo Capital Finance (UK) Limited, Stockholm Branch	Sweden
Wells Fargo Bank, National Association, DIFC Branch	Dubai, United Arab Emirates