WELLS FARGO

Europe, Middle East and Africa (EMEA)

Wells Fargo International Customer Privacy Notice

This notice applies to the United Kingdom ("**UK**"), countries in the European Union ("**EU**"), the Dubai International Financial Centre ("**DIFC**"), and the Kingdom of Saudi Arabia ("**KSA**").

Effective: 25 June 2025

Part 1. Introduction

What is this document and why should you read it?

"We", "our", "us", or "Wells Fargo" refers to the Wells Fargo entity listed in Part 4 with which you or your organization have a relationship. As a data controller, Wells Fargo provides this privacy notice ("**Notice**") to describe our processing of information related to you ("**Personal Data**"). Wells Fargo may process your Personal Data where you or your organization have a relationship with us. As described below, we may also process your Personal Data where providing financial products and carrying out investment, treasury management, payment, and other financial services.

The "Wells Fargo Group" includes, in addition to the Wells Fargo entities listed in Part 4, different Wells Fargo affiliates across the globe ("**Affiliated Entities**"). Each Affiliated Entity, if not listed in Part 4, uses a different privacy notice to describe its practices and guide its processing activities. The privacy notices for those Affiliated Entities are available at www.wellsfargo.com/privacy-security. If you or your organization has a relationship or shares Personal Data with an Affiliated Entity that is not listed in Part 4, that separate privacy notice will govern the Personal Data provided to that Affiliated Entity, not this Notice. Even in that case, Personal Information shared with Wells Fargo is governed by this Notice.

What types of Personal Data do we collect?

Wells Fargo collects different types of Personal Data. In EMEA, we primarily have relationships and accounts with corporations and other legal entities. We may, however, collect information about individual representatives of our customer organizations ("**Customers**") or other individuals who have a connection with our Customers or our services (collectively, "**Individuals**"). This information may include:

- **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; 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 licence; 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.

IPN EU2511 (Rev 25/06/2025)

- **Financial data and payment details:** salary and other income; bank account details; sources of wealth; assets; financial relationships; and financial transactions.
- **Marketing and communications data:** marketing preferences and customer service interactions; responses to voluntary surveys; recordings of telephone calls with customer service and other representatives (to the extent permitted by law); and copies of electronic communications you provide to or receive from us.
- **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; data associated with verification of politically exposed persons; education history; professional memberships and qualifications; and other information contained in your curriculum vitae or resume.
- **Customer access or system usage data**: information given by completing forms and surveys as well as data about your use of our application systems, including authentication credentials such as usernames or IDs and passwords to log into portals or applications; location data; user display name and identifier; other website or product access information; and use of credit card.
- **Market data**: information from market research, any data obtained and opinions expressed when participating in any customer or market surveys.
- **Geographical data:** information about your location.
- **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, voicemail etc.
- **Complaints data:** data collected for the processing in relation to any Wells Fargo customer complaints procedures.
- **Regulatory data:** information we need to support our regulatory obligations.
- **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 use these technologies to recognize you, remember your preferences and tailor the content we provide to you.

Wells Fargo may also collect certain types of special category personal data as permitted and/or required by local law or with your explicit consent, such as health/medical information (collectively, "**Sensitive Personal Data**"). We collect this information for specific purposes, such as health/medical information in order to accommodate a disability or illness. As explained below, we will only use such Sensitive Personal Data for those purposes and as permitted by law.

Collectively, the above categories of data constitute Personal Data. We may collect Personal Data in various ways, such as where you enter into a transaction or contractual arrangement with us; participate in our programs or activities; provide data at industry events and trade shows; or visit our facilities.

We may also collect Personal Data when we visit you at your offices or when you contact our customer services or our personnel via email, instant messaging, and/or telephone; in connection with your inquiries and communications with us; or from other sources, including your employer, data companies, publicly accessible databases, and joint marketing partners.

When asked to provide Personal Data, you may decline. If, however, you choose not to provide the data that are necessary for us to operate the requested services, we may not be able to provide you with certain services.

Who are we?

Wells Fargo Group is one of the largest financial institutions in the world. As described in Part 2, in order to carry out our business operations, Wells Fargo and the Affiliated Entities need to process certain Personal Data of Individuals

and Customers. The financial product or service you or your organization is receiving or seeking to receive from the Wells Fargo Group determines which Wells Fargo entity listed in Part 4 is providing the service and is the primary controller of your Personal Data. Part 4 also lists each of those entities and their jurisdictions. Contact information for our EMEA Regional Privacy Officer is listed in Part 3.

Name of group parent: Wells Fargo & Company

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

Part 2. Our handling of Personal Data

Why do we process Personal Data?

Wells Fargo needs to process Personal Data for a number of purposes. A primary purpose is to ensure that we can provide Customers with our products and services, which they have requested. As described below, we also need to use Personal Data for purposes of carrying out our business operations, including confirming a person's authority as a representative or agent of a Customer, maintaining our relationship with you, manage risk, ensuring security, maintaining business continuity plans and processes, providing online services and platforms, improving or marketing our products and services, research and development, training staff, carrying out system or product development, prevent and detect crime including fraud and financial crime, undertaking internal investigations and audits, handling legal claims, responding to requests from regulatory authorities, and complying with applicable laws and regulations on a global basis.

In particular, we process the following Personal Data for the following purposes:

- **To provide and improve the performance of products and services requested by our Customers.** We may process general data, position or employment/work description, identification and authentication data, customer access or system usage data, financial data and payment details, marketing and communications data, market data, geographical data, investigation data, complaints data, regulatory data and background or credit check data in order to: perform obligations under our agreements; carry out related business functions; process data and transactions; perform commercial banking services (including deposit taking and account management); conduct credit checks and due diligence; market products and services; provide investment banking and financial services; improve the performance of our products and services; and manage Customer relationships, complaints and inquiries, including where we need to contact Customers or Individuals with important information or for other administrative purposes. We process such data because you voluntarily provide this information and give your consent for us to process it; 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.

- **To comply with legal or regulatory obligations and laws & regulations.** We may process any of the above-mentioned types of Personal Data for the purpose of meeting our monitoring, recordkeeping and reporting obligations (for instance, telephone call recording for legal and regulatory purposes), conducting audits, detecting, preventing and investigating fraud, preventing money-laundering, terrorism financing, and proliferation financing, including carrying out background checks; fulfilment of tax control and notification obligations, carrying out due diligence and know-your-customer (**KYC**) checks; identifying potential conflicts of interest; complying with sanction rules and anti-corruption, anti-bribery, and transparency obligations; responding to legal processes such as subpoenas; pursuing legal rights and remedies; defending litigation; conducting internal investigations; managing internal complaints or claims; and complying with internal policies or procedures. 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.

- **To confirm a person's authority as a representative or agent of a Customer.** We process general data, position or employment/work description, financial data and payment details, background or credit check data, identification and authentication data, customer access or system usage data and geographical data to confirm a person's authority as a representative or agent of a Customer with which Wells Fargo or its Affiliated

Entities have entered or intend to enter into various arrangements, including deposit contracts, loan contracts, contracts for foreign exchange transactions, contracts involving derivative transactions, letters of credit, loan services, account management, commercial banking, commercial real estate, structured lending, corporate and investment banking services, credit card issuance and processing, financial services, and investment management. 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.

- **To conduct record-keeping.** We process general data, position or employment/work description, financial data and payment details, background or credit check data, identification and authentication data, customer access or system usage data, market data, geographical data, complaints data, investigation data and regulatory data to facilitate the management of our records in a systematic manner so they can be retrieved when required for legal, regulatory or operational reasons. To the extent permitted by applicable law and regulation, Wells Fargo may record telephone calls to support meeting our legal, regulatory or compliance requirements 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.

- **To protect Legal Rights and fulfil Legal obligations.** We may process any of the above-mentioned types of Personal Data when we believe it is necessary or appropriate to enforce our terms and conditions and to protect our/your rights for privacy, safety or assets/property, and/or that of our Affiliates or others. 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.

- **For sale or business transaction**. We may process any of the above-mentioned types of Personal Data in connection with any reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or any portion of our business, assets or stock (including in connection with any bankruptcy or similar proceedings). We process such data 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.

Under which lawful bases do we rely on to process Personal Data?

Wells Fargo may process Personal Data:

- because you voluntarily provide this information and give your consent for us to process it;
- because this information 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;
- for insurance purposes;
- 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
- because this information is necessary to protect the vital interests of any person.

Do we transfer Personal Data to different countries?

The Wells Fargo Group operates across the globe, and we may transfer Personal Data to Affiliated Entities located in countries other than the country where a Customer opened its account or maintains its relationship with us. Transfers can also take place where the Wells Fargo Group engages third parties to assist with certain operations and activities, as they also may be established in different countries, including countries located outside the EU, the UK, the DIFC or the KSA respectively. The countries where the Wells Fargo Group has operations are shown on the map at https://www.wellsfargo.com/cib/global-services/locations/.

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 herein 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 or the KSA 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, the DIFC or the KSA to countries not considered adequate by the relevant Data Protection Authority, we have put in place safeguards and adequate measures, such as standard contractual clauses as adopted by the EU, the UK, the DIFC or the KSA respectively to protect your Personal Data. Please contact our EMEA Regional Privacy Officer, using the contact information in Part 3, to obtain a copy of these safeguards and measures.

To whom do we disclose Personal Data?

We may disclose Personal Data for the purposes described in Part 2 to the following recipients:

- **Affiliated Entities.** Wells Fargo has Affiliated Entities and subsidiaries operating in the United States and around the world, including the group parent in the United States, Wells Fargo & Company, and Wells Fargo Bank, N.A. Wells Fargo may disclose Personal Data to our Affiliated Entities on a worldwide basis and our Affiliated Entities may use the data for the purposes described above and to the extent permitted by applicable law. In certain circumstances, an Affiliated Entity may be acting as an independent controller of processing of your Personal Data. If you have any questions, please contact our EMEA Regional Privacy Officer, using the contact information in Part 3.
- **Beneficiaries, counterparties, and other parties related to a transaction; credit reference agencies.** The Wells Fargo Group may disclose Personal Data to beneficiaries, counterparties, or other parties related to a transaction on a worldwide basis to provide the services requested by our Customers and to comply with legal obligations and regulations. We may provide Personal Data to credit reference agencies where permitted by applicable law.
- **Service providers.** The Wells Fargo Group may disclose Personal Data to information technology providers or other service providers around the world that act on our behalf and under our instructions regarding the processing of such data ("**Data Processors**"). Data Processors will be subject to contractual obligations to implement appropriate technical and organizational security measures to safeguard Personal Data and to process Personal Data only as instructed.
- **Regulators, Public and Governmental Authorities, and other Legally Authorized Recipients.** The Wells Fargo Group may disclose Personal Data if required or permitted by applicable law or regulation, including laws and regulations of the United States and other countries, or in the good faith belief that such action is necessary to: (a) comply with a legal obligation or in response to a request from law enforcement or other public authorities wherever the Wells Fargo Group may do business; (b) protect and defend the rights or property of any Wells Fargo Group entity; (c) act in urgent circumstances to protect the personal safety of Individuals, Customers, and contingent resources/employees of any Wells Fargo Group entity or other persons; or (d) protect against any legal liability. In addition, the Wells Fargo Group may share Personal Data with U.S. regulators and other self-regulatory bodies that are competent to oversee our operations, wherever the Wells Fargo Group may do business.
- **Acquiring Entities.** The Wells Fargo Group might sell, buy, restructure or reorganize businesses or assets. In the event of any actual or proposed sale, merger, reorganization, 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 the legal obligations to ensure their protection.
- **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 purposes described in Part 2, Personal Data may be shared with one or more professional advisors.

How do we keep your Personal Data safe?

We have implemented appropriate technical, physical and organizational security measures to safeguard Personal Data in accordance with the Wells Fargo's 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 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 our EMEA Regional Privacy Officer using the contact information in Part 3.

How long do we keep your 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 following:

- The length of time we have an ongoing relationship with you and provide the services to you (for example, for as long as your organization has an account with us or keeps using the services);
- Whether there is a legal obligation to which we are subject (for example, certain laws require us to keep records of your transactions for a certain period of time after your organization no longer has an account with us);
- Whether retention is advisable in light of our legal position (such as in regard to applicable statutes of limitations, litigation or regulatory investigations); and/or
- Whether our operational needs require maintaining your personal 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).

Do we use any Cookies and similar technologies?

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.

Part 3. 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 make a complaint in relation to these rights, contact our EMEA Regional Privacy Officer using the information below. We will respond to your request consistent with applicable law. 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 the following link(s):

United Kingdom	Information Commissioner's Office (ICO)
European Union	Our Members | European Data Protection Board (europa.eu)
DIFC	Data Protection | DIFC
KSA	Saudi Data & AI Authority | SDAIA | Data and AI

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 below. 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 the 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 below. 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.

How can you stop Wells Fargo from sending you marketing materials?

We will only send you marketing and sales materials where, and to the extent required by applicable law, you have consented to receive such materials. If you do not want to receive our marketing and sales materials by direct mail, telephone or email, please follow the unsubscribe or opt-out instructions provided in those communications or submit a written request to the EMEA Regional Privacy Officer using the address shown below. You can also contact our EMEA Regional Privacy Officer to exercise your right to object to the receipt of these communications. We will comply with any such request within a reasonable period after receipt.

How can you exercise your rights?

At Wells Fargo, we have team members who are dedicated to responding to requests in relation to your Personal Data, and to helping you with any other questions. For the Wells Fargo entities listed in Part 4, please contact our EMEA Regional Privacy Officer using the contact information below:

Europe, Middle East, and Africa:
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

Can we modify 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.

Part 4. Wells Fargo entities operating in EMEA

One of these EMEA entities listed below will be the controller of your Personal Data, based upon your or your organization's relationship with the Wells Fargo Group. You should consult your organization or contact at the Wells Fargo Group to determine the name of the entity or entities with which you or your organization have a relationship.

A list of entities in the Wells Fargo Group operating in EMEA is set out 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