INTERNATIONAL PRIVACY NOTICE

Introduction	This International Privacy Notice (hereinafter this "**notice**") describes how we will use your personal data. This notice relates to the use of personal data obtained to run our business and provide you with products and services. It covers the processing of personal data whether or not you (or an entity that you own or control) become a customer and includes any processing of personal data before you apply for a product or service. For purposes of this notice, personal data is data which by itself, or with other data available to us, can be used to identify individuals (natural persons) like you. Banco Santander International ("**we**", "**us**" and "**our**"), which also uses the brand name "**Santander Private Banking**," is the data controller. You can contact Banco Santander International's Data Protection Officer (DPO) at 1401 Brickell Avenue, Suite 1500 - Miami FL 33131, USA, +1 (305) 530-2900 or at privacy@bpi-gruposantander.com, if you have any questions.
The types of personal data we collect	Whether or not you (or an entity that you own or control) become a customer, we will collect your personal data from you directly or from third parties, including governmental and other public sources. We will collect most of this data directly from you during the account application process. Such personal data may include: • Name and personal details, including contact information (e.g. home and business address and address history, email address, home, business and mobile phone numbers). • Date of birth and/or age. • Financial details (e.g. salary and other income, and accounts held with other providers). • Records of products and services you have obtained or applied for. • When using services like our e-banking platform or mobile, applications, the relevant technology used to access or manage them (e.g. mobile phone location data, IP address, MAC address). • Biometric data (e.g. fingerprints and voice recordings for TouchID and voice recognition). • Information from credit reference or fraud prevention agencies, court records of debt judgments and bankruptcies and other publicly available information. • Family information (e.g. number of dependents). • Education and employment details/employment status. • Personal data about other named applicants. • Information on any trust, company or other vehicle that you may have established for wealth management purposes, including Personal Investment Companies. • Contact details and information about your business.
Monitoring of communications	Subject to applicable law, we will monitor and record your calls, emails, text messages, social media messages, e-banking, videoconferences and other communications relating to your dealings with us. We will do this for regulatory compliance, self-regulatory practices, crime prevention and detection, to protect the security of our communications systems and procedures, to check for obscene or profane content, for quality control and staff training. We may also monitor activities on your account where necessary for these reasons. Such monitoring is justified by our legitimate interests or our legal obligations.
Using your personal data: the	Local data protection law imposes certain obligations on us as to how we process your personal data, which vary depending on where you reside (e.g., European Union, Brazil). This means we must have one or more legal bases to process your personal data. The most common legal bases that apply to our

legal bases and purposes	use of your personal data are outlined below (noting that these legal bases are different depending on where you reside).[1] • As necessary **to perform our contract with you** for the relevant account, product or service. Such examples include but are not limited to: - Taking steps at your request prior to entering into a contract; - Deciding whether to enter into a contract with you; - Managing our contract with you; - Updating our records; - Providing you with trade confirmations and account statements; - Contacting you about your account; and - Recovering debts owed to us. • As necessary **for our own legitimate interests** or those of other persons. Such examples include but are not limited to: - For good governance, accounting, and managing and auditing our business operations; - Searching credit reference agencies if you apply for credit; - Monitoring emails, calls, other communications, and activities on your account; - Referring you for services at our affiliates; - Booking travel, accommodation or related services on your behalf for client events; - For market research, analysis and developing statistics; and - Sending you marketing communications. • As necessary **to comply with a legal obligation and/or to exercise rights in judicial, administrative or arbitration proceedings**. Such examples include but are not limited to: - For compliance with legal and regulatory requirements; - When you exercise rights under data protection law and make data subject requests; - For the establishment and defense of legal rights; - For activities relating to the prevention, detection and investigation of crime; - Verifying your identity, and conducting fraud prevention and anti-money laundering checks; and - Monitoring emails, calls, other communications, and activities on your account. • Based **on your consent**. Such examples include but are not limited to: - When we process any special categories of personal data about you at your request (e.g., biometric data,); and - When you request that we disclose your personal data to other people or organizations. **You are free to deny or, at any time, to change your mind and withdraw your consent. However, the consequence of such action might be that we can't provide you with certain services.**
Sharing of your personal data with third parties	Subject to applicable data protection law we may share your personal data with third parties. The following is an illustrative list of third parties that may receive your personal data.

[1] This is not intended to be an exhaustive discussion of the legal bases applicable in each jurisdiction.

	• Banco Santander S.A., Santander group companies and associated companies in which we have shareholdings and employees, officers, agents or professional advisors of these companies. • Sub-contractors and other persons who help us provide our products and services, including vendors that prepare and distribute monthly account statements. • Companies and other persons providing services to us. • Our legal and other professional advisors, including our auditors. • Fraud prevention agencies, credit reference agencies, and debt collection agencies. • Other organizations who use shared databases for income verification and affordability checks and to manage/collect arrears; • Government bodies and agencies in the US and overseas; • Courts, to comply with legal requirements, and for the administration of justice. • Other parties where necessary in an emergency or to otherwise protect your vital interests. • Other parties where necessary to protect the security or integrity of our business operations. • Other parties connected with your account (e.g. directors,. shareholders, beneficial owners or any named official who will see your transactions). • Other parties when we restructure or sell our business or its assets or have a merger or re-organization. • Market research organizations who help to improve our products or services. • Payment systems (e.g. American Express, Visa or MasterCard). If we issue cards linked to your account, such payment systems may transfer your personal data to others as necessary to operate your account and for regulatory purposes, to process transactions, resolve disputes and for statistical purposes, including sending your personal data overseas. These third parties may be considered our processors, independent or joint controllers, under applicable data protection law. You may request further information on this as stated below under “Your rights under applicable data protection law” below.
International Transfers	Your personal data may be transferred outside of the European Union or Brazil or elsewhere. To the extent required by applicable law, steps will be necessary to safeguard your data if transferred to a jurisdiction that does not offer an adequate level of protection as provided by your country of residence. These include imposing contractual obligations upon the recipient to protect your personal data or requiring the recipient of your personal data to subscribe or be certified with an “international framework” of protection.
Data anonymization and aggregation	Your personal data may be converted into statistical or aggregated data which cannot be used to identify you. Once anonymized and/or aggregated, this is not considered to be personal information under applicable law.
Identity verification and fraud prevention checks	The personal data we’ve collected about you might be shared with fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify your identity. If fraud is detected or suspected, you could be refused certain services. We may also search and use our internal records for these purposes. We may also hold personal information you give to us (e.g., name, address, date of birth, nationality, etc.) to undertake periodic due diligence checks which banks are required to undertake to comply with applicable legislation and regulation.

Automated decision making and processing	Automated processing and decision making involves processing your personal data without human intervention to evaluate your personal situation such as your economic position, personal preferences, and interests. We may do this to decide what marketing communications are appropriate for you and to decide which of our other products or services might be of interest to you. All this activity is on the basis of our legitimate interests, to protect our business, and to develop and improve our products and services. If E.U.'s General Data Protection Regulation (GDPR) is applicable, you have a right not to have a decision made based solely on automated processing (including profiling) that produces legal or similar significant effects on you. However, this does not apply where the processing is necessary for entering into, or the performance of, a contract between us, is authorized by law, or where you have given your consent to the processing (though you may revoke your consent thereafter).
Your marketing preferences and related searches	We will use your address, phone numbers, and email address, and other personal details you provided to us, to contact you regarding products and services that we offer. **You can opt-out of marketing communications at any time by contacting us at optout@bpi-gruposantander.com.** Such marketing efforts are within our legitimate interests.
Criteria used to determine retention periods (whether or not you become a customer)	The following criteria are used to determine data retention periods for your personal data: • *Retention in case of queries*. We will retain your personal data as long as necessary to deal with your queries (e.g. if your application is unsuccessful). • *Retention in case of claims*. We will retain your personal data for as long as you might legally bring claims against us. • *Retention in accordance with legal and regulatory requirements*. We will retain your personal data after your account, policy or service has been closed or has otherwise come to an end based on our legal and regulatory requirements.
Your rights under applicable data protection law	Depending on jurisdiction where you reside, local data protection law may provide you certain rights The following is an illustrative list of the rights that may apply to you (noting that these rights don't apply in all circumstances): • The right to be informed about our processing of your personal data, including, in certain jurisdictions, the right to know with whom we share your personal data. • The right to have your personal data corrected if it is inaccurate and to have incomplete personal data completed ("right to rectification"). • The right to object to processing of your personal data, including the right to object to any data processing activity not based on your consent (if consent is required). • The right to restrict processing of your personal data. • The right to have your personal data erased (the "right to be forgotten"), including the right to have your personal data anonymized or restricted. • The right to request access to your personal data and information about how we process it ("data subject access requests"). • The right to move, copy or transfer your personal data ("data portability"). • Rights in relation to automated decision making, including profiling. • The right to not give consent and to know the consequences arising therefrom and the right to withdraw your consent.

	For more details on all the above, or to exercise any of these rights (if applicable), you can contact us at privacy@bpi-gruposantander.com or at the phone number or address provided at the beginning of this notice. If you are a resident of the European Union, you have the right to complain to your local data protection regulator or the Spanish Data Protection Agency (www.agpd.es), our Lead Supervisory Authority. Brazilian residents may contact the ANPD, the Brazilian data protection regulator (https://www.gov.br/anpd/pt-br). Residents of other jurisdictions may contact the relevant privacy regulator.