

Privacy Notice - Brazil

EFFECTIVE FROM 6 JANUARY 2023

WHO IS THIS NOTICE ISSUED BY AND WHAT INFORMATION DOES IT PROVIDE?

The purpose of this notice is to explain how we “process” or use your personal data, to help you understand why we collect, use, store, share, and secure your data, and to explain your privacy rights.

This notice is issued by JPMorgan Chase & Co. and its branches, subsidiaries and affiliates identified as controllers in Schedule A, you can access this section by clicking [here](#) if you are viewing the document electronically. In this notice, we use “J.P. Morgan” “we”, “us” or “our” depending on context.

This notice uses certain defined terms:

- **“Controller”** is an entity that decides how and why personal data is processed and is usually responsible for complying with applicable data protection laws.
- **“Data Protection Authority”** is the public authority that is responsible for protecting, supervising and enforcing compliance with the Brazilian Data Protection Law.
- **“Personal Data”** is information that is about any individual, or from which any individual is identifiable. It can be anything from your name to your IP address. You can see what Personal Data we collect [here](#).
- **“Process, processed or processing”** encompasses the collection, use, storage and analysis of data, among others. The principle covers anything that is done with any personal data, whether or not by automated means.
- **“Processor”** means any person or entity that processes Personal Data on behalf of the Controller (other than employees of the Controller).
- **“Sensitive Personal Data”** is personal data on racial or ethnic origin, religious belief, political position, membership in a trade union or affiliation to religious, philosophical or political organization, data concerning health or sexual life, genetic or biometric data, when linked with an individual under the Brazilian Data Protection Law.

This notice is designed to supplement any specific terms and conditions that may be applicable to your relationship with us. If you have any questions about the role of this document and how it applies to your personal data, you should speak to your J.P. Morgan team.

WHO SHOULD READ THIS NOTICE?

This notice is addressed to people with whom we interact. This includes:

- visitors to our websites (our “**Sites**”);
- customers (including prospective customers, our customers’ advisors, family office staff or other associated professional advisors or consultants);
- people connected with the customer as professional advisors, consultants, family office staff, directors, interns, secondees or officers;
- representatives of an account holder (such as holders of a power of attorney or other appointed third parties);
- vendors;
- anyone who calls our services centers or who writes to us via post, email or social media, and
- other recipients of our services (together, “**you**”).

In some cases, this will apply to the personal data of third parties. You can see more details [here](#).

HOW WILL WE UPDATE THIS NOTICE?

This notice may be amended and updated from time to time to reflect changes such as the categories of data that we collect, process and share or to reflect any changes in applicable law. We encourage you to regularly check this page, and we will include the effective date in order to help you check whether or not there have been any changes since you last accessed the notice.

WHAT SHOULD I DO IF I HAVE ANY QUESTIONS?

If you have any comments, questions or concerns that are not addressed in this notice, you can contact your regular J.P. Morgan client service contact, or the following central contacts:

- **Brazil:** ipb.brazil.privacy.control@jpmorgan.com or via post at Avenida Brigadeiro Faria Lima 3729, Floor 12, São Paulo, 04538-905, Brazil.
- **Switzerland:** WM.Switzerland.Privacy.Controls@ jpmorgan.com or via post at 35 Rue du Rhône, 1204 Geneva, Switzerland.
- **Latin America and Global Families Group:** GFG.LATAM.GDPR.Inbox@jpmorgan.com or via post at 390 Madison Avenue, Floor 30, New York, NY 10017.

You may also contact J.P. Morgan’s Data Protection Officer for Brazil, Solange Mendonca, at Brasil.DPO@jpmchase.com or via post at Avenida Brigadeiro Faria Lima 3729, Floor 10, São Paulo, BR-SP, 04538-905, Brazil.

OUR APPROACH TO DATA PROTECTION

Data Security: We have implemented appropriate technical and organizational security measures designed to protect your Personal Data. We protect your data in line with our global security program built on our core principles of only using the data required for the processing in question, controlling access to systems and datasets to those who need to use the data, and using an encryption and anonymization process to secure the data that we hold in our systems. You are responsible for ensuring that any Personal Data you send to us are sent securely.

Data Accuracy: We take reasonable steps designed to ensure that any Personal Data we process are accurate and, where necessary, kept up-to-date and that any of your Personal Data that we process that are inaccurate (having regard to the purposes for which they are processed) are erased or rectified without delay. From time to time, we may ask you to confirm the accuracy of your Personal Data.

Data Minimization: We take reasonable steps designed to ensure that your Personal Data we process are limited to the Personal Data reasonably required in connection with the purposes set out in this notice.

HOW DO WE COLLECT PERSONAL DATA?

We collect Personal Data in a number of different ways. This table sets out the methods by which we collect your Personal Data, with some examples.

HOW WE COLLECT PERSONAL DATA	EXAMPLES
When you provide us with personal data	• When you fill out an account opening form. • When you communicate with us via email (or any other electronic channels), phone call or letter. • If another party to your account provides us with Personal Data. • If you make a complaint or provide feedback, including any data that you share with us or that we receive as a part of our investigation into your complaint or feedback.
When you use our services	• Transactions on your account, such as requesting a credit facility or your investment in our funds.
Search, social media and publically available data sources	• Public social media profiles, such as LinkedIn or Bloomberg. • Search engine results and news reports from available sources, including Google and Bloomberg. • Any public entry on electoral registers, company registers or local equivalents.
From third parties who provide it to us	• If we carry out any checks via credit reference agencies. • If we request confirmation of your employment from your employer. • If you purchase any of our products and services from a third party. • Government and law enforcement authorities.

HOW WE COLLECT PERSONAL DATA	EXAMPLES
When you visit or use any of our Sites	• If you give us your details in order to set up an online account with us. • When visiting a Site, your device and browser may automatically disclose certain information (such as device type, operating system, browser type, browser settings, IP address, language settings, dates and times of connecting to a Site and other technical communications information).

Although your provision of personal information to us in connection with this notice is voluntary (unless we inform you otherwise), we may be unable to provide you with our products/services (or any part thereof) or comply with any applicable laws or regulations or guidelines and codes issued by regulatory or other authorities if you do not do so.

HOW DOES THIS NOTICE APPLY TO THIRD PARTY PERSONAL DATA?

If you transfer third-party Personal Data to us, this notice will also apply to that Personal Data.

If you supply us with the Personal Data of third parties, you will be responsible for informing those third parties that their Personal Data has been transferred to us and for informing them that this notice will apply. You are also responsible for the collection and recording of their consent, if necessary.

In addition, if such Personal Data is considered as confidential under applicable law, you are responsible for ensuring that the third parties have waived any applicable confidentiality requirements. You are also responsible for the collection and recording of their consent, if consent is required by law and such obligation is legally imposed to you.

WHEN DO WE RECORD OUR INTERACTIONS WITH YOU?

In some circumstances we will record, monitor and retain communications (including facsimile, telephone conversations, email, instant messaging, your interaction with our Sites and any other electronic communications), including those held between you and/or your agent and employees of

J.P. Morgan. These records and recordings are made for the purposes of ensuring compliance with J.P. Morgan's legal and regulatory obligations and internal policies.

All such records will be the sole property of J.P. Morgan and will be accepted by you as conclusive evidence of the orders, instructions or conversations recorded, if applicable.

WHAT PERSONAL DATA DO WE COLLECT, GENERATE AND USE?

This table sets out the categories of personal data that we collect and generate. The type and amount of data that we collect and generate will differ depending on your relationship with us, and the services that we provide to you.

PERSONAL DATA COLLECTED, GENERATED AND USED	EXAMPLES
Personal details	• Your name, including any previous names, preferred names or nicknames. • Your gender, date of birth, nationality and marital status. • Information concerning your identity, such as government-issued identification numbers. • Information about your lifestyle and social circumstances, and details of your education and qualifications. • Authentication data, such as your login details. • Identifying number allocated to you and used for validating electronic transactions, such as PINs. • Photographs and visual images, such as CCTV footage if you visit our offices, or images of identity documents obtained during onboarding. • Information relating to your personal appearance or behavior, such as how you interact with our services.
Contact details	• Your address, telephone number, email address, and social media details.
Employment details	• The nature of your industry and current role, plus any other business activities. • The names of your current and former employers. • Any contact details relating to your work.

PERSONAL DATA COLLECTED, GENERATED AND USED	EXAMPLES
Financial details	- Your billing address and bank account numbers. - Your instruction records, transaction details, and counterparty details. - Your total assets and overall financial position. - The fact that you have a banking relationship with J.P. Morgan Private Bank.
View and opinions	- Any views and opinions that you choose to send to us or make public. - Any views and opinions about us that you choose to send to us or make public.
Electronic identifying data	- IP addresses, geolocation data, online identifiers (including in relation to your device) and cookies. - Data relating to your use of our Sites, such as browsing activity or transaction logs.
Personal data of third parties	Any of the above in relation to other parties such as family members, dependents, friends, employees and advisors.
Others	Any other personal data we receive from you (or on your behalf), including voice recordings or files (e.g. documents, audio files or video files) received via electronic communication channels.

If we collect Personal Data relating to your race or ethnicity, political opinions, religious or philosophical beliefs, trade union membership, physical or mental health, sexual life, genetic or biometric data, or any other information that may be deemed to be sensitive under applicable law, we will only process this data for specific purposes and taking into consideration the legal basis established by applicable law.

The table below sets out some examples of when we might process Sensitive Personal Data.

SENSITIVE PERSONAL DATA COLLECTED, GENERATED AND USED	EXAMPLES
Race or ethnicity	We may request this information from you when you apply for one of our services, and subsequently process this information for the purposes of a legal obligation (e.g., diversity reporting).
Political opinions and religious or philosophical beliefs	You may agree to share your beliefs with us or make them public. Alternatively, we may become aware of them during the administration of your account when we carry out checks required for the detection and prevention of crime, or if necessary for the establishment, exercise or defense of legal rights.
Health information	You may tell us your health information in order to ensure that you can use our services, such as any dietary requirements you may have.
Sensitive personal data of third parties	Any of the above in relation to other parties such as family members, dependants, friends, employees and advisors.

WHEN DO WE SHARE PERSONAL DATA WITH THIRD PARTIES?

We will share your Personal Data in some circumstances, such as with other members of the J.P. Morgan group and third-party service providers who act on our instructions under legal agreements to assist us in providing our products and services. Some third parties who we share your data with process the data as independent controllers in their own right and in accordance with their own privacy policies.

For example, we may engage a third-party company to provide software to enable electronic signatures, or to process votes in connection with any securities that you may hold with us. You should be aware that once your data are shared with third parties, they may also be under a legal or regulatory duty to share that information, in some cases by making that data public.

WHO WE SHARE YOUR DATA WITH	EXAMPLES
Other entities within the J.P. Morgan group	- We may share your Personal Data for our internal operational purposes (e.g., in connection with our anti-money laundering obligations). - We may share your Personal Data that we processed for the purposes of Know Your Client checks if you wish to purchase products and services from another J.P. Morgan company. - In limited circumstances and subject to appropriate controls, we may share your Personal Data with our affiliates in order to assess whether or not some of their products and services are suitable for you, or to market products and services to you.
Your representatives and associates, including other parties who hold roles in relation to the same account relationship	- If another individual has authority over your account, we may disclose your personal data to them in order to operate your account. - If you supply us with Personal Data relating to a member of your family, we may have to share that Personal Data with account authorities where we need to do so in order to meet our legal obligations and/or operate your account.
Third-party service providers who provide services to us, including their sub-contractors or delegates	- We may share your Personal Data with payment services providers, where we need to do so in order to satisfy a payment request that you make. - If we hold your assets in custody as part of the services that we provide, we may share your data with third-party companies who support the market infrastructure. - We may share your Personal Data with data aggregation services if you choose to use them, or if it is in our legitimate interests to do so. - We may share information with fund administrators or other service providers in order to assist them in complying with their legal obligations, such as Know Your Client checks. - We may share your personal information with relevant communication or social media channel providers or platform hosting service providers if you choose to use them, or if it is in our legitimate interest to do so. - Debt-collection agencies and tracing agencies. - Credit reference agencies. - Anti-fraud services.
J.P. Morgan's professional advisors	We may share personal data with our accountants, auditors, financial advisors, lawyers and other outside professional advisors.
Third-party plug-in providers	Our Sites may use third-party plug-ins or content. If you choose to interact with any such plug-ins or content, your Personal Data will be shared with the third-party provider of the relevant social media platform. We recommend that you review that third party's privacy policy before interacting with such plug-ins or content.
Any relevant third-party acquirer(s)	- If we sell or transfer all or a portion of our business or assets. - If we reorganize, dissolve or liquidate all or a portion of our business or assets.
Governmental, legal, regulatory or similar authorities	- If they require us to share your Personal Data. - If we are required to report any actual or suspected breach of applicable law or regulation. - Any relevant party to the extent necessary for the establishment, exercise or defense of legal rights. - Any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties.
Other third parties	- Any relevant party to the extent necessary for the establishment, exercise or defence of legal rights. - Any relevant party for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Our Sites may use third-party plug-ins or content. If you choose to interact with any such plug-ins or content, your Personal Data may be shared with the third-party provider of the relevant social media platform. We recommend that you review that third party's privacy policy before interacting with its plug-ins or content.

If we engage a third-party Processor to process your personal data, the Processor will be subject to binding contractual obligations to: (i) only process the Personal Data in accordance with our prior written instructions; and (ii) use measures to protect the confidentiality and security of the Personal Data; together with any additional requirements under applicable law.

SHARING YOUR PERSONAL DATA INTERNATIONALLY

Because of the international nature of our business, we may need to transfer your Personal Data within the J.P. Morgan group, and to third parties, in connection with the purposes set out in this notice. For this reason, we may transfer your Personal Data to other countries that may have different laws and data protection compliance requirements, including data protection laws of a lower standard to those that apply in the country in which you are located.

Where we transfer your Personal Data to other countries, we do so on the basis of:

- adequacy decisions;
- our Binding Corporate Rules;
- suitable Standard Contractual Clauses; or
- other valid transfer mechanisms.

If you want to receive more information about the safeguards applied to international transfers of personal data, please contact us using the details provided in ‘What should I do if I have questions?’ or by clicking [here](#), if you are viewing this document electronically.

HOW LONG DO WE RETAIN YOUR PERSONAL DATA FOR?

We will retain your Personal Data in line with our data retention policy and for the minimum period required. The duration of the retention period is determined by a number of criteria, including the nature of our relationship with you, the relevant jurisdiction, the type of data, and the products and services that the data relates to.

We will retain your Personal Data for as long as we have an ongoing relationship with you—for example, if you are a client, or a recipient of one of our mailing lists—or where we need to retain the Personal Data in connection with the lawful purposes set out in this notice and we have a valid legal basis for doing so. In the event of a legal claim, we may continue to process your Personal Data for such period as is necessary in connection with that legal claim.

After this period, we will typically retain your Personal Data for any additional limitation period (i.e., any period during which a legal claim could be raised) plus an additional reasonable period of time after the end of the limitation period, in order to ensure that the data can be used in connection with any legal claim that may be brought. During the legal hold period, we will restrict our processing of your Personal Data to the storage of, and maintaining the security of, the data, except to the extent that the data need to be reviewed in connection with any legal claim, or any obligation under applicable law.

Once we no longer need to retain your Personal Data, we will either:

- permanently delete or destroy the relevant Personal Data;
- archive your Personal Data so that it is beyond use; or
- anonymize the relevant personal data.

YOUR LEGAL RIGHTS

Subject to applicable law, you may have certain rights in relation to your data, and we want to make sure that you can exercise them. In some cases, however, we may not be able to continue to provide you with certain products and services or continue to operate your account.

To exercise one or more of these rights, or to ask a question, please contact us.

This does not affect any other rights that you may have under an agreement or applicable law.

YOUR RIGHTS	DESCRIPTION
Confirmation of processing	You have the right to know whether we process your Personal Data.
Access	You have the right to request copies of the Personal Data that we process or control. You have the right to know what Personal Data we collect and/or process, and how we use and disclose it. To do so, you should submit a Subject Access Request by contacting us here.
Rectification	If you believe that the Personal Data we process or control are incom-plete or inaccurate, you have the right to request rectification.

YOUR RIGHTS	DESCRIPTION
Elimination of data processed with consent	You have the right to request that we delete your Personal Data if we originally requested your consent to process the Personal Data and you wish to withdraw it.
Restriction	You have the right to request, on legitimate grounds, that we restrict the processing of your Personal Data we process or control.
Anonymization, blocking, elimination	You have the right to request anonymization, blocking or elimination of your Personal Data that are unnecessary, excessive or processed in a manner that is non-compliant with applicable law.
Portability	Under some circumstances, you have the right to receive your Personal Data in a readable format. You may also, under some circumstances, ask us to send your Personal Data in a readable format to a third party; however, we will not be responsible for what such third party does with your Personal Data, and you should ensure that you check any terms or privacy arrangements they have in place.
Objection	You have the right to object, on grounds relating to your particular situation, to the processing of your Personal Data by us or on our behalf.
Consent	If we have asked for your consent in order to process your Personal Data, you have the right to withdraw that consent.
Complaints	You have the right to complain to the appropriate Data Protection Authority regarding the processing of your Personal Data, either by us or on our behalf.

HOW DO WE USE COOKIES ON OUR SITES?

A cookie is a small file that is placed on your device when you visit a website (including our Sites). It records information about your device, your browser and, in some cases, your preferences and browsing habits. We may process your Personal Data through cookie technology, in accordance with our Cookie Policy (<https://www.jpmorgan.com/global/cookies>) or any other policy that we make available to you.

We will analyze the cookie data collected by us to improve the website and our services to you. The data collected will be stored in our systems and protected with the same degree of security used for all other client information.

DIRECT MARKETING

We may process your personal data to contact you, primarily by mail and email (and other electronic communication channels) and also on occasion by telephone, so that we can provide you with information concerning products and services that may be of interest, provided that we have first obtained your consent, to the extent required by, and in accordance with, applicable law.

If you do not wish to receive marketing communications from us, you can opt out at any time by contacting your regular J.P. Morgan contact, or by electronically unsubscribing from emails we have sent to you. After you unsubscribe, we will not send you further promotional messages, but we may continue to contact you to the extent necessary for the purposes of any services you have requested.

SCHEDULE A – DATA CONTROLLERS

For the purposes of this notice, the relevant Controllers are:

JPMORGAN CHASE & CO. ENTITY	CONTACT DETAILS
Banco J.P. Morgan S.A. J.P. Morgan Corretora de Câmbio e Valores Mobiliários S.A. J.P. Morgan S.A.—Distribuidora de Títulos e Valores Mobiliários JPMorgan Chase Bank, National Association (Brazilian branch) J.P. Morgan Administradora de Carteiras Ltda.	Avenida Brigadeiro Faria Lima, 3729, 04538-905, São Paulo, Brazil
J.P. Morgan (Suisse) SA	35 Rue du Rhône, 1204 Geneva, Switzerland
JPMorgan Chase Bank, N.A.	270 Park Avenue, New York, NY 10017, USA
J.P. Morgan Securities LLC	383 Madison Avenue, New York, NY 10179, USA

As the case may be, the above list shall also include any other present or future entity of the JPMorgan Chase & Co. group in Brazil. If you are unsure as to who the Controller of your Personal Data is, please contact us [here](#).

SCHEDULE B—PURPOSES FOR WHICH WE MAY PROCESS YOUR PERSONAL DATA (AND SENSITIVE PERSONAL DATA, AS PERMITTED), AND LEGAL BASIS FOR PROCESSING

The purposes for which we may process Personal Data, subject to applicable law, and the legal basis on which we may perform such processing, are:

PROCESSING PURPOSE	LEGAL BASIS FOR PROCESSING
Anti-money laundering/Know Your Client checks: Fulfilling our regulatory compliance obligations, including “KYC” checks; and confirming and verifying individuals’ identities (including by using credit reference agencies); and screening against government, supranational bodies and/or law enforcement agency sanctions lists, as well as internal sanctions lists and other legal restrictions.	• The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purposes of preventing money laundering, sanctions violations and protecting against fraud (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • We may carry out the processing when necessary to prevent fraud and your safety in the identification and authentication process of registration in electronic systems; or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).
Client on-boarding: On-boarding new clients; and compliance with our internal compliance requirements, policies and procedures. Information required to open and administer accounts includes, without limitation, the ultimate beneficial ownership, personal identification details or, for legal entities, country of incorporation/citizenship, residence, registered address or address of record, documentation required by us for the purposes of conducting Know Your Client, and anti-money laundering and counter-terrorism financing identification and verification, and any information relating to tax status.	• The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of on-boarding new clients (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • We may carry out the processing when necessary to prevent fraud and your safety in the identification and authentication process of registration in electronic systems; or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).

PROCESSING PURPOSE	LEGAL BASIS FOR PROCESSING
Credit worthiness: Conducting credit reference checks and other financial due diligence.	• The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of conducting financial due diligence (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • We may carry out the processing when necessary to prevent fraud and your safety in the identification and authentication process of registration in electronic systems; or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).
Provision of products and services to you: Administering relationships and related services, including attendance at events and granting you direct access to investment research; performance of tasks necessary for the provision of the requested services; communicating with you in relation to those services.	• The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of providing products and services to you (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • We may carry out the processing when necessary to prevent fraud and your safety in the identification and authentication process of registration in electronic systems; or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).
Marketing / Prospecting: Evaluating whether or not the products and services of any of our affiliates (or other J.P. Morgan clients) may be of interest to you, and providing you with marketing information concerning such products and services, by mail, email, SMS, social media, post, telephone or in person, unless you have specifically instructed us not to do so, and subject to ensuring that such communications are provided to you in compliance with applicable law; maintaining and updating your contact information where appropriate; and communicating with other current or potential clients, including by disclosing to them the fact that J.P. Morgan provides services to you.	• We have a legitimate interest in carrying out the processing for the purpose of conducting marketing and prospecting (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).
Operation of our Sites: Operation and management of our websites; providing content to individuals; displaying advertising and other information to individuals; and communicating and interacting with you via our websites.	• The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of operating our websites (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • We may carry out the processing when necessary to prevent fraud and your safety in the identification and authentication process of registration in electronic systems; or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).

PROCESSING PURPOSE	LEGAL BASIS FOR PROCESSING
IT operations: Management of our communications systems; operation of IT security; and IT security audits.	• The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We may carry out the processing when necessary to prevent fraud and your safety in the identification and authentication process of registration in electronic systems; or • We have a legitimate interest in carrying out the processing for the purpose of managing and operating our IT systems and ensuring the security of those systems (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
Health and safety: Health and safety assessments and record keeping; and compliance with related legal obligations.	• The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of providing a safe and secure environment at our premises (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • The processing is necessary to protect the life or the physical safety of any individual.
Financial management: Sales; finance; corporate audit; and vendor management.	• The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of managing and operating the financial affairs of our business (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).
Research: Conducting market or customer satisfaction research; and engaging with you for the purposes of obtaining your views on our products and services.	• We have a legitimate interest in carrying out the processing for the purpose of conducting research and producing analysis (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).
Security: Physical security of our premises (including records of visits to our premises and CCTV recordings); and electronic security (including log-in records and access details, where you access our electronic systems).	• The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of ensuring the physical and electronic security of our business, premises and assets (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We may carry out the processing when necessary to prevent fraud and your safety in the identification and authentication process of registration in electronic systems.
Investigations: Detecting, investigating and preventing breaches of policy, and criminal offenses, in accordance with applicable law.	• The processing is necessary for compliance with a legal obligation; or • We have a legitimate interest in carrying out the processing for the purpose of detecting, and protecting against, breaches of our policies and applicable laws (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • The processing is necessary to protect the life or the physical safety of any individual.
Legal compliance: Compliance with our legal and regulatory obligations under applicable law.	• The processing is necessary for compliance with a legal obligation.

PROCESSING PURPOSE	LEGAL BASIS FOR PROCESSING
Legal proceedings: Establishing, exercising and defending legal rights.	• The processing is necessary for compliance with a legal obligation; or • The processing is necessary for the regular exercise of rights in court or in administrative or arbitration proceedings; or • We have a legitimate interest in carrying out the processing for the purpose of establishing, exercising or defending our legal rights (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations.
Improving our products and services: Identifying issues with existing products and services; planning improvements to existing products and services; and creating new products and services.	• The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We have a legitimate interest in carrying out the processing for the purpose of improving our products or services (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).
Risk Management: Audit, compliance, controls and other risk management.	• The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • We have a legitimate interest in carrying out the processing for the purpose of managing risks to which our business is exposed (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms).
Fraud prevention: Detecting, preventing and investigating fraud.	• The processing is necessary for compliance with a legal obligation; or • The processing is necessary in connection with any contract that you may enter into with us, or to take steps prior to entering into a contract with us; or • We carry out the processing for the protection of credit, including situations prior to or after granting credit to you, as well as for credit limit assessment and management and collection activities, among other situations; or • We may carry out the processing when necessary to prevent fraud and your safety in the identification and authentication process of registration in electronic systems; or • We have a legitimate interest in carrying out the processing for the purpose of detecting, and protecting against, fraud (to the extent that such legitimate interest is not overridden by your interests or fundamental rights and freedoms); or • We have obtained your prior consent to the processing (this legal basis is only used in relation to processing that is entirely voluntary—it is not used for processing that is necessary or obligatory in any way).