SANTANDER LONDON BRANCH - GENERAL DATA PROTECTION NOTICE

1. Introduction

Your personal data is data which by itself, or with other data available to Santander London Branch (a branch of Banco Santander, S.A.) (collectively referred to as "we/us/our" (hereinafter, "**Santander London Branch"**) in this Data Protection Notice), can be used to identify you. Santander London Branch is the data controller for the uses of your personal data. This Data Protection Notice (or "**Notice**") sets out how we (either alone or jointly with others) will determine the purposes and means of processing your personal data. You can contact our Santander London Branch Data Protection Officer (DPO) at our principal place of business located at 2 Triton Square, Regents Place, London, NW1 3AN, or through the following email, SLBPrivacy@santandercib.co.uk., if you have any questions.

This Notice sets out how we may use, if you are an individual, your personal data or, if you are a corporate, partnership or other entity, the personal data of your directors, partners, legal representatives, advisors, employees, guarantors, shareholders, beneficial owners, and other individuals connected with you, which may be required to facilitate the relationship between us and our ability to offer you products/services. It covers the processing of personal data, whether the entity you represent becomes a client or not, also applying to prospect clients, and includes any processing of personal data before applying for a product and/or service.

If you are a listed representative or contact person of an entity in the process of contracting products or services from Santander London Branch, it is your responsibility to have the appropriate legitimation for the contribution of personal data. You assume the responsibility of informing the entity whom you represent of the terms set out below, exempting Santander London Branch of any responsibility in this regard. Santander London Branch may carry out periodic checks to verify this fact, carrying out due diligence measures in accordance with the data protection regulations.

2. The categories of personal data we collect and use

The categories of personal data we capture and use will depend on the purpose for which you are entering into a relationship with Santander London Branch, or for what purpose you are accessing our website. We will use your personal data for some or all of the reasons set out in this Notice. If the entity you represent becomes a client, we will use it to manage the product and/or service you have applied for on behalf of the entity. We will collect most of this directly during the application process. Examples of the personal data we collect and use in relation to our relationship or this website may include:

Where you are representing a prospective client:

- Direct identification and identifying personal data: Your full name and personal details, including contact information (e.g. residential and business address and address history, passport number, email address, business and mobile phone numbers, date of birth and/or age);
- Customer information data: where applicable and relevant, we might process records of products and/or services you have previously obtained on behalf of the entity you represent (these are recorded in internal systems);
- Financial information and information from third parties: information from government and law enforcement agencies (UK and Overseas) credit reference agencies or fraud

prevention agencies, electoral roll, court records of debt judgements and bankruptcies and other publicly available sources. Financial situation information as well as information on any financial associates you may have; tax information.

- Education and employment data: employment details or employment status for fraud prevention purposes;
- Criminal records information: we might also processes criminal records information for compliance with legal obligations.

3. Providing your personal data

In relation to any application you make on behalf of the entity you represent including onboarding, you state that the data provided to Santander London Branch is accurate and authentic, agreeing to inform any modification or variation to Santander London Branch.

With regards to all personal data requested by Santander London Branch, we will tell you if providing some personal data is optional, including if we ask for your consent to process it. Unless otherwise specified, you must provide all personal data requested by us so that we can process any application and provide the service you require. If you or the entity you represent decline to provide certain data it may prove impossible to proceed with the operation.

4. Monitoring of communications

Subject to applicable laws, we may monitor and record your calls, emails, text messages, social media messages and other communications relating to your dealings with us. We will do this for regulatory compliance, self-regulatory practices, crime prevention and detection purposes, to protect the security of our communications systems and procedures, to check for obscene or profane content, for quality control and staff training, and when we need to access records of communications between us.

We may also monitor activities associated with the product and/or service we provide the entity you represent for these reasons. In relation to the legal basis for processing such personal data, this is justified by our legitimate interests or our legal obligations - for example, if we have reason to believe that a fraud or other crime is being committed, and/or where we suspect non-compliance with anti-money laundering regulations to which we are subject.

5. Using your personal data: the legal basis and purposes

Santander London Branch may perform its data processing activities itself or through a third party, keeping in any case the duty of secrecy.

We will process your personal data:

A) As necessary to perform our **contract** with you for the relevant product and/or service we provide or receive, e.g.:
   I. To take steps at your request prior to entering into it;
   II. To decide whether to enter into it;
   III. To manage and perform that contract; and
   IV. To update our records.

All personal data provided to Santander London Branch by a client, service provider or supplier within this purpose is legitimated on the execution of pre-contractual measures or, whether appropriate, on the execution of the contractual relationship during the term in which the legal

relationship remains enforceable and, even later, until the expiration of the limitation period of the eventual liability claims required by the current regulation.

With regards to the control of the identity of the authorized signatures provided by our client or supplier in the on boarding process, all personal data provided to Santander London Branch within this purpose, is legitimated on the execution of pre-contractual measures or, whether appropriate, on the execution of the contractual relationship during the term in which the legal relationship remains enforceable and, even later, until the expiration of the limitation period of the eventual liability claims required by the current regulation.

If the client or supplier's legal representatives authorize another person to exercise their rights in relation to this contract on its behalf, Santander London Branch informs the authorized person to this effect that their personal data provided to us in the scope of this contractual relationship will be processed by Santander London Branch, which may process such personal data, directly or through third parties acting on its behalf, and always without prejudice to the duty of secrecy, for the purposes of the maintenance, development, management and control of that contractual relationship.

B) As necessary for our own **legitimate interests** or those of other persons and organisations, for example:
   I. For good governance, accounting, managing and auditing our business operations;
   II. To carry out searches at credit reference agencies (if you are over 18);
   III. For market research, analysis and developing statistics; and
   IV. To send marketing communications related to events and conferences organised by us, in relation to our business or to products or services similar to those your entity has contracted with us.

C) As necessary to comply with a **legal obligation**, for example:
   I. When you exercise your rights under Data Protection law and make requests;
   II. For compliance with legal and regulatory requirements and related disclosures;
   III. For the establishment and defence of legal rights;
   IV. For activities relating to the prevention, detection and investigation of crime;
   V. To verify your identity, make credit, fraud prevention, anti-money laundering and KYC checks;
   VI. To monitor emails, calls, other communications, and activities on the products and/or services we provide to the entity you represent; and
   VII. For the management of possible conflicts of interest that may arise.

To perform any action against fraud through scoring techniques and expert analysis, among others, with the objective of analysing the level of risk, our client or supplier commits to provide all the necessary personal data, including those of its legal representatives, agents, advisors and contacts based on a legitimate interest recognized by the regulators of Santander London Branch.

To perform any anti-money laundering action and other regulatory issues our client or supplier commits to provide all the necessary data, including those of its legal representatives, directors, and contacts to comply with this purpose based on the compliance of legal obligations, included in anti-money laundering and counter terrorist financing laws concerning national security.

D) Based on your consent, for example:

Your consent might be obtained for the processing of your personal data that requires such consent. You are free at any time to change your mind and withdraw your consent. The consequence might be that we cannot do certain things for you.

6. Sharing of your personal data

Subject to applicable Data Protection law, we may share your personal data with, but not limited to:

- The Santander group of companies and associated companies in which we have shareholdings and employees, officers, agents or professional advisors of these companies (Banco Santander, S.A. and any of its branches; Santander Corporate & Investment Banking is a brand name used by Banco Santander, S.A., and its affiliates, including Santander UK plc);
- Other Financial Institutions;
- Sub-contractors and other persons who help us provide our products and services; Companies and other persons providing products and/or services to us;
- Our legal and other professional advisors, including our auditors;
- Fraud prevention agencies and credit reference agencies when we open the product and/or service and periodically during the service management to the entity you represent;
- Government bodies and agencies in the UK and overseas (e.g., HMRC, who may in turn share it with relevant overseas tax authorities and with regulators e.g., the Prudential Regulation Authority, the Financial Conduct Authority, the Information Commissioner's Office);
- 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 the product and/or service 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-organisation;
- Market research organisations who help to improve our services;
- External sources of publicly available information such as Companies House, credit reference agencies; and other internal insight; and
- Anyone else, where we have your consent, or as required by law.

7. International transfers

Given the international dimension of the Santander group of companies, your personal data may be transferred outside the UK for the same purposes indicated in section 5 above. While some countries have adequate protections for personal data under applicable laws, in other countries steps will be necessary to ensure appropriate safeguards apply to it. These include imposing contractual obligations of adequacy or requiring the recipient to subscribe or be certified with an 'international framework' of protection.

Safeguards can include, but are not limited to:

- The Standard Data Protection Clauses such as the Model Contract Clauses.
- Binding Corporate Rules or other contractual arrangements, provided the recipients in other countries have obtained the requisite approvals. The published list of approvals is available here: https://ico.org.uk/for-organisations/binding-corporate-rules.
- Using any one other statutory exceptions, if any available. Making our own assessment of the adequacy of the level of protection for the rights of data subjects.

8. Your marketing preferences

We may use your personal data to submit to you, on behalf of the entity you represent, communications related to events and conferences organised by us, in relation to our business or to products or services similar to those your entity has contracted with us. The attendance to these events is always voluntary and may require additional registration by you. We will do this based on Santander London Branch's legitimate interest.

If you wish to opt out of receiving this marketing communications related to our events and conferences, you can do so at any time by sending an email to slbprivacy@santandercib.co.uk.

9. Criteria used to determine retention periods (whether or not you become a client)

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;
- Retention in case of claims. We will retain your personal data for as long as you might legally bring claims against us; and
- Retention in accordance with legal and regulatory requirements. We will retain your personal data after the service contracted by the entity you represent has been closed or has otherwise come to an end based on the legal and regulatory requirements.

10. Your rights under applicable Data Protection law

This section lists the various data protection rights that you have. Your personal data is protected under Data Protection legislation, and consequently you have a number of rights that you can enforce against us as your data controller. Except for the exercise of rights of access request for which we would require specific content and format, as covered below, you may exercise your rights covered in this section at any time by sending a written communication attaching a copy of your ID or official document proving your personal identification to: SLBPrivacy@santandercib.co.uk. Please note that these rights do not apply in all circumstances.

Your rights include:

- **The right to be informed -** the right to be informed means we must provide you information about how we might process your personal information. We do this through this document.
  The right of rectification – you have the right to have your personal data corrected if it is inaccurate and to have incomplete personal data completed in certain circumstances.
- **The right to object** - in some cases, you have the right to object to processing of your personal data. This right allows you to object to processing based on legitimate interests, direct marketing and processing for purposes of statistics, including the anonymization of your personal data for statistical and aggregated use.

- **The right to restrict processing** – you have the right to restrict processing of your personal data by blocking or supressing processing in the following circumstances: Where you contest the accuracy of the personal data, you can request we restrict processing until you have verified the accuracy of the personal data. Where you have objected to processing and we are considering whether our legitimate interests override yours. Where our processing of your personal data was unlawful but you wish us to restrict processing instead of erasing the data. Where we no longer need the personal data but you ask us to retain it in connection with establishing, exercising or defending a legal claim.
- **The right to erasure** - (also known as the '**right to be forgotten'**). This right is not absolute – it applies only in particular circumstances, where it does not apply any request for erasure will be rejected. Circumstances when it might apply include: where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed; if the processing is based on consent which you subsequently withdraw; when there is no overriding legitimate interest for continuing the processing; if the personal data is unlawfully processed; or if the personal data has to be erased to comply with a legal obligation. Requests for erasure will be refused where its retention is lawful and permitted under Data Protection law, for instance where the personal data has to be retained to comply with legal obligations, or to exercise or defend legal claims.
- **The right of access** – this right enables you to **request access** to the personal data held about you and to obtain certain prescribed information about how we process it. This is more commonly known as submitting a 'data subject access request'. This right will enable you to obtain confirmation that your personal data is being processed, to obtain access to it, and to obtain other supplementary information about how it is processed. In this way you can be aware of, and you can verify, the lawfulness of our processing of your personal data.
- **The right to data portability** – you have the right to **move, copy or transfer** certain personal data. Also known as 'data portability'. You can do this where we are processing your personal data based on consent or a contract and by automated means. Please note that this right is different from the right of access (see above), and that the types of data you can obtain under these two separate rights may be different. You are not able to obtain through the data portability right all of the personal data that you can obtain through the right of access.
- **The rights in relation to some automated decision-making** about you, including profiling. Santander Corporate & Investment Banking do not undertake automated decision making or processing therefor this right is not applicable to our clients.

To formally request any right of access or 'data subject access request' your request must be submitted in writing to the SLB Data Protection Officer, Santander London Branch, 2 Triton Square, Regents Place, London, NW1 3AN or at slbprivacy@santandercib.co.uk.

Your request must be submitted in writing to the email or address above via a signed letter containing the following information:

- ✓ Your full name
- ✓ Date of birth
- ✓ Address and previous address where relevant
- ✓ A daytime phone number in case we need to contact you to discuss your request

October 2022

- ✓ Your client reference number
- ✓ Your relationship with us for example if you are a director or shareholder of the client company you represent
- ✓ Any other relevant information

You also have the right to lodge a complaint with the Information Commissioner's Office (ICO), the UK's independent body empowered to investigate whether we are complying with the Protection law. You may do this without prejudice to any other administrative appeal or judicial action You can do this if you consider that we have infringed the legislation in any way. You can visit ico.org.uk for more information.

If you wish to exercise any of your rights against us, we will explain whether or not those rights do or do not apply to you with reference to the above, and based on the precise circumstances of your request.

When sending personal data to us we strongly advise you to secure your communication e.g. by password protecting email attachments.

11. Identity verification and fraud prevention checks

We will perform credit and identity checks with one or more credit reference agencies. The personal data we have collected from you at application or at any stage may be shared with fraud prevention agencies to prevent fraud and money-laundering and to verify your identity, and they will give us information about you. If fraud is detected, the entity you represent could be refused financing and/or other certain services and products

We may also search and use our internal records for these purposes. We may also hold all the information you give to us (i.e. name, address, date of birth, nationality) to conduct periodic due diligence checks, which banks are required to undertake to comply with UK legislation.

When we process your personal data, we do so on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us. Such processing is also a contractual requirement of the services or financing you have requested.

We may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.

Fraud Preventing Agencies can hold your personal data for different periods of time, and if you are considered to pose a fraud or money laundering risk, your data can be held for up to six years from its receipt.

Consequences of processing

If we determine that you pose a fraud, threat to national security or money laundering risk, we may refuse to provide the services, goods or financing you have requested, or we may stop providing existing services and products to you, on behalf of the company you represent. This may, also, result in other organisations refusing to provide you with products and/or services.

Credit reference agencies

When we carry out a search at the credit reference agencies, they will place a footprint on your credit file. This footprint will be viewable by other lenders and may affect your ability to get credit elsewhere. (A credit search is not carried out if you are under 18).

We will also continue to exchange information about you on behalf of the entity you represent with credit reference agencies while your entity has a relationship with us. The credit reference agencies may in turn share your personal information with other organisations.

The personal data shared with the credit reference agencies will relate to you. Details about you in relation to the application of the entity you represent (whether it is successful) will be recorded.

Records of searches with credit reference agencies will be retained by them based on their legal and regulatory requirements. A financial association link between yourself and any named business partner or individual will be created at the credit reference agencies. This will link your financial records and be taken into account in all future applications by either or both of you until either of you apply for a notice of disassociation with the credit reference agencies.

If you are a director, we will seek confirmation from the credit reference agencies that the residential address that you provide is the same as that shown on the restricted register of directors' usual addresses at Companies House.

The identities of the credit reference agencies, and the ways in which they use and share personal information is explained in more detail via the credit reference agency Information Notice (CRAIN) document which can be accessed via any of the following links: experian.co.uk/crain equifax.co.uk/crain transunion.co.uk/crain

Data transfers within fraud prevention agencies

Where fraud prevention agencies transfer your personal data outside of the UK, they impose contractual obligations on the recipients of that data, in order to protect your personal data to the standard required in the UK.

They may also require the recipient to subscribe to 'international frameworks' intended to enable secure data sharing.

For more information about the fraud prevention agencies that we use, and how they will process your personal data, please contact:

The Compliance Officer
Cifas
6th Floor, Lynton House 7-12
Tavistock Square
London
WC1H 9LT
Email: compliance@cifas.org.uk
Website: cifas.org.uk/privacy-notice

The Compliance Officer
National Hunter
PO Box 2756
Stoke on Trent
Staffordshire
ST6 9AQ
Website: nhunter.co.uk/howitworks/

The Compliance Officer

October 2022

National Cira
Sinectic Solutions Limited
Sinectics House
The Brampton Newcastle under Lyme
ST5 0QY
Website: synectics-solutions.com/Data-Protection

Additional information on credit reference agencies.

The identities of the credit reference agencies, and the ways in which they use and share personal information is explained in more detail in the credit reference agency Information Notice (CRAIN) document, which can be accessed via any of the following links:

- experian.co.uk/crain
- equifax.co.uk/crain
- transunion.co.uk/crain