Using My Personal Data

August 2018

Santander
Corporate & Investment Banking

How we use your personal data

When you apply for a financial service with Santander Corporate & Investment Banking (SCIB) you can access a Data Protection Statement explaining how we treat your personal data. This is available at santandercib.co.uk

This document provides you with further information and details of your personal data rights under the General Data Protection Regulation.

Contents

1. SCIB Data Protection Statement explained

Data Protection Statement section	Explanation
Introduction	This section sets out who the Data Controller is and provides contact details for the Data Protection Officer. In legal terms SCIB is designated as the Data Controller because it is the entity that (either alone or jointly with others) determines the purposes and means of processing your personal data. If you have any questions about how your personal data is used, or the information included in this booklet, our Data Protection Officer (DPO) can be contacted at 201 Grafton Gate East, Milton Keynes, MK9 1AN.
The types of personal data we collect and use	The type of personal data we collect and use will vary depending on the services you require or have and the nature of your relationship with us, for example if you are a Director or Shareholder of the client company.
Providing your personal data	This section states that you will be told whether the provision of your personal data is optional or mandatory. If provision of the data is mandatory then you will need to provide the information so that we can process your application and provide the service you require.
Monitoring of communications	This section explains why we may monitor or record your on-going communications with us, for example; calls, emails and text messages. We monitor our communications with you so that we comply with regulatory rules and our own internal processes or protocols. We do this: ■ Where it is relevant to the services we provide; ■ To prevent or detect crime; ■ In the interests of protecting the security of our communications systems and procedures; ■ For quality control and staff training purposes; and ■ When we need to access these as a record of what we have said to you/what you have said to us. For example, where we are required by Financial Conduct Authority (FCA) regulations to record certain telephone lines, we will do so. Our monitoring will also check for obscene or profane content in communications. In very limited circumstances we may conduct short-term and carefully controlled monitoring of activities on your service. This will only be done where this is justified by our legitimate interests, or to comply with 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.

Using My Personal Data

Data Protection Statement section	Explanation
Using your personal data: the legal basis and purposes	This section describes how your personal data may be used, and the legal basis for the processing of your information. The legal basis for us processing or analysing your personal data will depend on what we're trying to achieve. Data Protection legislation allows us to process your personal data for our own legitimate interests - provided those interests do not override your own interests and/or your fundamental rights and freedoms. An example of 'legitimate interests' would be where we share your personal data within the Santander group for administrative purposes. Complying with established legal obligations is another reason for us to share your personal data. For example where we are required to provide periodic reporting to regulators. You may also give your consent for us to process personal data at your request, an example of this would be where you ask us to pass your personal data to a third party which is acting on your behalf to provide you with a service. Under Data Protection legislation you can withdraw your consent at any time. Withdrawal of consent may affect our ability to fulfil your request, as in the previous example, but will not affect our ability to deliver the service you have applied for where processing is based on your/our legitimate interests, our legal/ regulatory obligation, or it is necessary to perform a contract with you.
Sharing of your personal data	This section details when personal data may be shared and the types of people/organisations it can be shared with. We may share your personal data with the Santander group of companies and other persons providing services to us. This may include data back-up and server hosting providers, our IT software and maintenance providers and/or their agents. Further details of who we may share your personal data with are contained in the SCIB Data Protection Statement available at santandercib.co.uk Santander Corporate & Investment Banking is a brand name of Santander UK plc (which also uses the brand name Santander Corporate & Commercial Banking). The Santander group companies that we may share personal data with include Banco Santander, S.A.; Santander UK plc (including cahoot); Santander ISA Managers Ltd; Abbey Stockbrokers Ltd; Santander Asset Finance plc; Alliance & Leicester Personal Finance Ltd; Cater Allen Ltd (Cater Allen); Santander Asset Management UK Ltd; Santander Consumer (UK) plc; Santander Insurance Services UK Ltd; Santander Unit Trust Managers UK Ltd. You have the right to object to the sharing of your personal data where this sharing is based on your consent or in certain circumstances where the processing is based on our legitimate interests.
International transfers	This section explains that where we transfer your personal data outside of the UK and European Economic Area (EEA) appropriate safeguards will be put in place to protect that data Safeguards can include: (i) The Standard Data Protection Clauses (also known as EU Model Clauses), You can obtain a copy of these by contacting our Data Protection Officer (DPO) (ii) The US Privacy Shield and details are available here: privacyshield.gov/welcome or from our Data Protection Officer (DPO) (iii) Binding Corporate Rules, provided the recipients in other countries have obtained the requisite approvals. The published list of approvals is available here: ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm or from our Data Protection Officer (DPO)
Data anonymization and aggregation	Your personal data may be anonymised so it cannot identify you, then converted into statistical or aggregated data which may be used, for example, for statistical research and reports. This anonymised data may also be shared with the types of people/organisations covered under 'sharing of your personal data'. You have the right to object to the anonymization and subsequent processing of your personal information, where this activity is not based on your/our legitimate interests or our legal/regulatory obligations.
Identity verification and fraud prevention checks	This section explains that your personal data can be used to check your identity and for fraud prevention and anti-money laundering purposes. To find out more, refer to the 'Fraud prevention agencies explained' section of this booklet.

Data Protection Statement section	Explanation
Credit reference checks	This section provides information on the sharing of your personal data with the credit reference agencies. To find out more, refer to the 'Credit reference agencies explained' section of this booklet.
Automated decision making and processing	This section explains what automated decision making and processing is and our approach. Automated decision making involves processing your personal data without human intervention to evaluate your personal situation such as your economic position, personal preferences, interests or behaviour. Santander Corporate & Investment Banking does not undertake automated decision making or processing.
Your marketing preferences	This section tells you how we may use your information for marketing and market research purposes. Santander Corporate & Investment Banking will only contact you regarding information on our corporate products we believe may be of interest to you via the business contact details (e.g. email, address or telephone number) you have given us. You can tell us at any if you do not want to receive such marketing or market research requests.
Criteria used to determine retention periods	If you open an account or service with us, your information will be kept after your account or service is closed in accordance with our record retention policy. Further information can be found in our Data Protection Statement.
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 as a consequence you have a number of rights that you can enforce against us as your Data Controller. Please note that these rights do not apply in all circumstances. Your rights include: ■ The **right to be informed** - including about how we might process your personal data. This information is contained in the Data Protection Statement. ■ To have your personal data **corrected if it is inaccurate** and to have **incomplete personal data completed** in certain circumstances. ■ The right in some cases 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 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 **have your personal data erased** in certain circumstances (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. ■ 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. ■ **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. ■ **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. 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 Data Protection law. 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 that or those rights do or do not apply to you with reference to the above, and based on the precise circumstances of your request.

2. Fraud prevention agencies explained

Before we provide a financial service to you, we are required to undertake a number of checks - not only to verify your identity, but also to prevent fraud or money laundering. These checks require us to process your personal data.

What we process and share

The personal data we process and share includes data you have provided to us and/or data we have received from third parties. This may include your:

- Name
- Date of birth
- Business and residential address and address history
- Contact details, such as corporate email addresses and telephone numbers
- Tax and passport numbers
- Financial information
- Employment details
- Identifiers assigned to your computer or other internet connected device including your Internet Protocol (IP) address
- Vehicle details

When we and fraud prevention agencies 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 and/or the fraud prevention agencies may also enable law enforcement agencies to access and use your personal data to detect, investigate and prevent crime.

FPAs 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.

Consequences of processing

If we, or a fraud prevention agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services, goods or financing you have requested, or to employ you, or we may stop providing existing services to you.

A record of any fraud or money laundering risk will be retained by the fraud prevention agencies, and may result in others refusing to provide services to you.

Automated decision making and profiling

The GDPR has provisions on:

- Automated individual decision-making (making a decision solely by automated means without any human involvement);and
- Profiling (automated processing of personal data to evaluate certain things about an individual).

SCIB does not use automated decision making or profiling.

Data transfers

Where fraud prevention agencies transfer your personal data outside of the European Economic Area (EEA), they impose contractual obligations on the recipients of that data, in order to protect your personal data to the standard required in the EEA. 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
National Cira
Sinectic Solutions Limited
Sinectics House
The Brampton
Newcastle under Lyme
ST5 0QY

Website: synectics-solutions.com/Data-Protection

3. Credit reference agencies explained

When we process an application for a service, we will perform standard credit and identity checks on you with one or more credit reference agencies.

In doing this we will supply your personal information to the credit reference agencies and they will give us information about you. This will include information from your credit application, information about your financial circumstances and your financial history. The credit reference agencies will supply to us information that is in the public domain (including the electoral register), and shared credit, financial, and fraud prevention information.

We'll use this information to:

- Assess your creditworthiness;
- Verify the accuracy of the data you've provided to us;
- Prevent criminal activity, fraud and money laundering; and
- Manage your service(s).

We'll continue to exchange information about you with the credit reference agencies while you have a relationship with us. This information may be supplied to other organisations via the credit reference agencies.

When the credit reference agencies receive a search from us, they will place a search footprint on your credit file that may be seen by other lenders.

If you are making a joint application, or tell us that you have a spouse or financial associate, we'll link your records together - so you should make sure you discuss the application with them in advance, and share this information with them before making the application. The credit reference agencies will also link your records together, and these links will remain on your and their files until such time as you or your partner successfully file for a 'disassociation' with the credit reference agencies to break that link.

For more information about the credit reference agencies that we use and how they will process your personal data, including the Credit Reference Agency Information Notice (CRAIN), please contact:

Call Credit
Address Callcredit Information Group, One Park Lane, Leeds, West Yorkshire, LS3 1EP

Phone no 0330 024 7574

Website: callcredit.co.uk/crain

Equifax
Address Equifax Ltd, Customer Service Centre, PO Box 10036, Leicester, LE3 4FS

Phone no 0333 321 4043 or 0800 014 2955

Website: equifax.co.uk/crain

Experian
Address Experian, PO Box 9000, Nottingham, NG80 7WF

Phone no 0344 481 0800 or 0800 013 8888

Website: experian.co.uk/crain

4. Your personal data rights explained

Your personal data is protected under Data Protection legislation, and as a consequence you have a number of rights that you can enforce against us as your Data Controller. When sending personal data to us we strongly advise you to secure your communication e.g. by password protecting email attachments.

Right to be Informed	The right to be informed means we must provide you information about how we process your personal data. We do this through this booklet and the Data Protection Statement. The type of personal data we collect and use will vary depending on the services you require or have and the nature of your relationship with us, for example if you are a Director or Shareholder of the client company.
Contact	santandercib.co.uk
Right to Rectification	The right to have your personal data corrected if it's inaccurate, or to have any incomplete personal data completed.
Contact	Your Relationship Manager Client Services at CMS.CorporateUK@santandercib.co.uk
Right to Object	The right to object to processing of your personal data based on legitimate interests, direct marketing and processing for purposes of statistics.
Contact	Your Relationship Manager Client Services at CMS.CorporateUK@santandercib.co.uk
Right to Restrict Processing	The right to restrict processing of your personal data by blocking or supressing processing in certain circumstances (see section one for further detail).
Contact	Your Relationship Manager Client Services at CMS.CorporateUK@santandercib.co.uk
Right to Erasure	Also known at the Right to be Forgotten, The broad principle underpinning this right is to enable you to request the deletion or removal of your personal data where there is no compelling reason for its continued processing.
Contact	Your Relationship Manager Client Services at CMS.CorporateUK@santandercib.co.uk
Right of Access	The right to access your personal data and supplementary information. This right also allows you to be aware of and verify the lawfulness of the processing. Your request may be submitted verbally, by email or in writing and should provide the information below. ■ 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 ■ Your personal reference number (P number) ■ Your relationship with us for example if you are a director or shareholder of the client company ■ Any other relevant information
Contact	Subject Access Requests, Santander UK plc, PO BOX 1111, Bradford, BD1 9NQ Your Relationship Manager Client Services at CMS.CorporateUK@santandercib.co.uk
Right to Data Portability	The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
Contact	Your Relationship Manager Client Services at CMS.CorporateUK@santandercib.co.uk

Complaints	We always strive to provide you with the best products and services. Unfortunately things can sometimes go wrong, but telling us about errors or oversights will give us the chance to fix things for you and make long-term improvements to our services. You may also be able to refer your complaint to the Financial Ombudsman Service. The Financial Ombudsman Service acts as an independent and impartial organisation which helps settle disputes between consumers and financial services businesses.
Contact	Your Relationship Manager Client Services team, Santander UK plc, 2 Triton Square, Regent's Place, London, NW1 3AN. Email: clientservice@santandercib.co.uk Or telephone 0207 756 6666 financial-ombudsman.org.uk

Glossary of terms

Binding Corporate Rules: Personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or a group of enterprises engaged in a joint economic activity

Data Controller: The natural or legal person, public authority, agency or other body which along or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Protection Officer: A person charged with advising the controller or processor on compliance with data protection legislation and assisting them to monitor such compliance.

Disassociation: A disassociation is a method of removing a financial connection between individuals that have been connected together as financial associates at the credit reference agencies. When people have joint accounts or they live together where their earning and spending behaviour affects each other, information on these financial relationships is taken into account when individuals apply for credit. Credit reference agencies hold this information as 'financial associations'. If an individual has been incorrectly linked to someone else or all financial ties have been broken so there are no longer any shared finances such as income or spending, then an individual can request for a 'disassociation' at the credit reference agencies.

EEA: The European Economic Area (EEA) is the area in which the Agreement on the EEA provides for the free movement of persons, goods, services and capital within the European Single Market, including the freedom to choose residence in any country within this area. The EEA includes the EU countries as well as Iceland, Liechtenstein and Norway.

Legal Basis: The legal basis for processing personal data.

Legitimate interest: The lawful grounds for data processing. Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject.

Personal data: 'Personal data' means any information relating to an identified or identifiable natural person ('Data Subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Processing: Processing means any operation or set of operations which is performed on personal data or on sets of personal data, where or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

US Privacy Shield: The framework for transatlantic exchanges of personal data for commercial purposes between the European Union and the United States, providing companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the EU and Switzerland to the United States.