

Using my personal data

How we use your personal data

When you applied for a financial product or service with Santander you would've been given a Data Protection Statement, explaining how we would treat your personal data.

This booklet provides you with more information about this, together with details of your personal data rights.

Contents

The Data Protection Statement explained	2
Fraud prevention agencies explained	5
Your personal data rights explained	6
Glossary of terms	9

1. The Data Protection Statement explained

Data Protection Statement section	Explanation
Introduction	<p>This section explains who the Data Controller is and provides contact details for the Data Protection Officer.</p> <p>In legal terms Santander UK plc is designated as the Data Controller because it's the entity that (either alone or jointly with others) determines the purposes and means of the processing of your personal data.</p> <p>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 Data Protection Officer, Santander, Sunderland, SR43 4GP.</p>
The types of personal data we collect and use	<p>The sort of personal data we collect and use will vary depending on the products or services you need or have, and your preferred relationship with us. For instance, biometric data will be captured if you register your fingerprints for Mobile Banking.</p>
Whether providing your personal data is required by law or contract or not	<p>This section states that you'll be told whether the provision of your personal data is optional or mandatory.</p> <p>If the provision of the data is mandatory and we don't already hold it, then you'll need to provide the information so that we can process your application or service.</p>
Monitoring of communications	<p>This section explains why we may monitor your on-going communications with us.</p> <p>This includes us monitoring our communications with you so that we comply with regulatory rules, or our own internal processes and protocols:</p> <ul style="list-style-type: none"> ◦ relevant to our business and 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've said to you or what you've said to us. For example, where we're required by Financial Conduct Authority (FCA) regulations to record certain telephone lines we'll do so. <p>Our monitoring will also check for obscene or profane content in communications.</p> <p>In very limited and controlled circumstances we may conduct short-term and carefully controlled monitoring of activities on your account or service. This will only be done where this is necessary for 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're subject.</p>
Using your personal data: the legal basis and purposes	<p>This section describes how your personal data may be used, and the legal basis for the processing of your information.</p> <p>The legal basis for us processing or analysing your personal data will depend on what we're trying to achieve.</p> <p>Data Protection legislation allows us to process your personal data for our own legitimate interests - provided those interests don't override your own interests and/or your fundamental rights and freedoms.</p> <p>An example of 'legitimate interests' would be if you believed you were the victim of a fraud or scam, and you asked us to investigate your claim. To understand what has happened we may need to share your name and account number, the details of any payment(s) made and details of the case with the other bank(s) involved. This is so they could trace transactional activity, help to recover any of your monies that may remain and reduce the opportunity of the funds being used to support criminal activity. Therefore, the sharing of your data with the bank(s) involved falls within your legitimate interests as well as ours - to ensure that funds are prevented from being used for fraudulent and/or money laundering activities.</p> <p>Please note: The bank(s) we may share your data with may be located outside of the UK or European Economic Area (EEA), and therefore may not be subject to the same data privacy legal obligations as banks within the UK or EEA.</p> <p>Complying with established legal obligations is another reason for us to share your personal data. For example if you need us to transfer funds via CHAPS or internationally, your personal data may be provided to overseas authorities and the beneficiary bank to comply with applicable legal obligations and to prevent crime. This may require us to share your personal data outside of the UK or EEA. This information may include your full name, address, date of birth and account number.</p> <p>Under Data Protection legislation you can withdraw your consent at any time. If you do this, and if there's no alternative lawful reason that justifies our processing of your personal data for a particular purpose, this may affect what we can do for you. For example, it may mean that if you have arrears on your account, we can't take into account any personal data concerning your health, which may result in us being unable to provide you with a service that you had requested.</p>

Data Protection Statement section	Explanation
Sharing of your personal data	<p>This section details when personal data may be shared, and the types of people/organisations it can be shared with.</p> <p>Where a joint account is converted into a sole account, information about the account and historical transactions will be available to all current and any future account holders later added to the account.</p> <p>We may share your personal information with 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.</p> <p>If you ask another person or organisation to act on your behalf we'll share relevant personal information with them to help them to deal with your request. For example, if you refer a complaint about us to the Financial Ombudsman Service, we'll share relevant complaint information with them so that they can review your case. In some cases this may include special categories of personal data (i.e. data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, or data relating to health, sex life/sexual orientation) where it's relevant to the complaint.</p> <p>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; Santander Asset Finance plc; Alliance & Leicester Personal Finance Ltd; Cater Allen Ltd (Cater Allen); Santander Asset Management UK Ltd; Santander Consumer (UK) plc; Santander Corporate & Commercial, a brand name of Santander UK plc and of Santander Asset Finance plc; Santander Insurance Services UK Ltd and Asto Digital Limited.</p>
International transfers	<p>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.</p> <p>Safeguards can include:</p> <ul style="list-style-type: none"> (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) Binding Corporate Rules.
Identity verification and fraud prevention checks	<p>This section explains that your personal data can be used to check your identity and for fraud prevention and anti-money laundering purposes.</p> <p>To find out more, refer to the 'Fraud prevention agencies explained' section of this booklet.</p>
Credit reference checks	<p>This section provides information on the sharing of your personal data with the credit reference agencies.</p>
Your marketing preferences and related searches	<p>This section tells you how we may use your information for marketing and market research purposes. You can tell us at any time that you don't want to receive marketing or market research requests.</p> <p>You can provide your marketing preferences as part of your application, and amend them at any time via our Marketing Preference Centre.</p>
Using automated decision making to make decisions about me	<p>This section explains what automated decision making is, and the circumstances when it may take place.</p> <p>We may automatically process your personal data, without human intervention, to evaluate certain personal aspects about you (known as profiling).</p> <p>In particular, we may analyse or predict (among other things) your economic situation, personal preferences, interests or behaviour. This could mean that automated decisions are made about you using your personal information. For example, we might analyse certain customer demographics, account holdings and account behaviours (such as Direct Debits you have set up on your accounts including those which identify accounts and products such as credit cards and store cards which you hold with other providers/elsewhere) and look at details of transactions relevant to your accounts. We may also analyse events such as the maturity dates of your accounts and opening anniversaries.</p> <p>We'll use your personal data to assess lending and insurance risk. When we do automated decision making including profiling activity to assess lending and insurance risks, this will be performed on the basis of it being necessary to perform the contract with you or take steps to enter into that contract.</p> <p>In some instances we'll use automated processing and decision making, where relevant, to decide which of our other products or services might be suitable for you, as well as to produce a personalised price for insurance products, to provide an indication of the price prior to an application being made (please note, publicly available information about you and information about you from third party data sources such as, credit reference agencies, will also be used to provide you with an indication of the price). The personalised price would be presented to you in marketing communications and during contacts with Santander that might be suitable.</p> <p>We'll look at the types of accounts that you already have with us, as well as your age, where this is relevant to the product, we think you might be interested in. We'll also conduct behavioural scoring, including by looking at the accounts and products you already have with us and how they are being used, such as account turnover, arrears and other indications of financial difficulties. Where searches are carried out against publicly available data sources and credit reference agencies, these searches may appear on your credit report, but they will not affect your ability to get credit.</p>

Data Protection Statement section	Explanation
	<p>We'll use the information from this activity to:</p> <p>Decide which other products and/or services from us or the Santander Group of companies or other persons, might be suitable for you, and for which you might be eligible. These can include those products/ services that are offered by us, or by us in conjunction with our partners, or by the Santander Group of companies. This means that automated decisions and processing can help to determine what marketing communications you receive.</p> <p>In addition, when we provide a product or service to you, we take into account other personal data that we hold about you - including how you use this and other accounts you have with us, Santander Group companies or associated companies. We may use your personal data for statistical analysis and system testing. We do all this on the basis that we have a legitimate interest in protecting our business, to understand your needs and provide a better service to you, and to help us develop and improve our products and services.</p> <p>Where profiling is based on legitimate interests you have the right to object to that processing.</p> <p>You may have a right to certain information about how we make these decisions. You may also have a right to request human intervention and to challenge the decision.</p>
Criteria used to determine retention periods	<p>This section within the Data Protection Statement explains the criteria we use when deciding how long personal data needs to be retained.</p>
Your rights under applicable Data Protection law	<p>This section lists the various data protection rights that you have.</p> <p>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 don't apply in all circumstances. Your rights include:</p> <ul style="list-style-type: none"> ◦ The right to be informed - including about how we might process your personal data. This was provided to you 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 (as relevant). This right allows individuals in certain circumstances to object to processing based on legitimate interests, direct marketing (including profiling) and processing for purposes of statistics. ◦ The right in some cases to restrict processing of your personal data, for instance where you contest it as being inaccurate (until the accuracy is verified); where you consider that the processing is unlawful and where this is the case; and where you request that our use of it is restricted; or where we no longer need the personal data. ◦ 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, and where it doesn't 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's 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 that 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 when your account is open and where we're 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're 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 (as relevant) if this has a legal or other significant effect on you as an individual. This right allows individuals, in certain circumstances, to access certain safeguards against the risk that a potentially damaging decision is taken without human intervention. <p>To complain to 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.</p> <p>If you seek to exercise any of your rights against us we'll explain whether or not that or those rights do or don't apply to you with reference to the above, and based on the precise circumstances of your request.</p>

Data Protection Statement section	Explanation
Data anonymisation and aggregation	<p>This section explains that your personal data may be turned into statistical or aggregated data, data that can no longer identify you.</p> <p>Your personal data may be converted into statistical or aggregated data, which can't be used to identify you. We may share and sell such anonymised data including in an aggregated format, within and outside of the Santander group of companies, for statistical analysis, research and other business purposes. For example, sharing information about general spending trends in the UK to assist in research. The law says this isn't considered to be personal information after it has been anonymised and/or aggregated.</p>

2. Fraud prevention agencies explained

Before we provide financial services and/or financing to you, we undertake a series 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 is what you've provided us with, details we've collected from you directly, and/or information we've received from third parties. This may include your:

- Name
- Date of birth
- Residential address and address history
- Contact details, such as email addresses and telephone numbers
- Financial information
- Employment details
- Identifiers assigned to your computer or other internet connected devices, including your Internet Protocol (IP) address

When we and/or the fraud prevention agencies process your personal data, we do so on the basis that we have a legitimate interest in verifying your identity and preventing fraud and money laundering, in order to protect our business and to comply with legal requirements. Such processing is also a contractual requirement of the services or financing you've 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.

Fraud prevention agencies can hold your personal data for different periods of time. Check their privacy policies for further information.

Automated decision making

As part of our personal data processing procedures, decisions may be made by automated means. This means we may decide that you could pose a fraud or money laundering risk if:

- our processing reveals your behaviour to be consistent with money laundering or known fraudulent conduct, or is inconsistent with your previous submissions/activity; or
- you appear to have deliberately hidden your true identity.

You have certain rights in relation to automated decision making processes. To find out more, refer to the 'Your personal data rights explained' section of this booklet.

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 financial services or financing you've requested, 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, financing or employment to you.

Data transfers

Fraud prevention agencies may allow the transfer of your personal data outside of the UK. This may be to a country where the UK Government has decided that your data will be protected to UK standards, but if the transfer is to another type of country, then the fraud prevention agencies will ensure your data continues to be protected by ensuring appropriate safeguards are in place.

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

The Compliance Officer

Cifas

6th Floor, Lynton House
7-12 Tavistock Square
London
WC1H 9LT

Website: www.cifas.org.uk/fpn

The Compliance Officer

National Hunter

PO Box 4744
Stone
ST15 9FE

Website: nhunter.co.uk/howitworks/

The Compliance Officer

National SIRA

Synetics Solutions Limited
Synetics House
The Brampton
Newcastle under Lyme
ST5 0QY

Website: synectics-solutions.com

3. 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.

If you're a Santander Corporate & Commercial customer and would like to discuss your personal data rights contact your Relationship Team or refer to the following relevant section of this booklet.

Right to rectification

This right refers to having your personal data corrected if it's inaccurate, or to have any incomplete personal data completed.

To request a right to rectification you can contact us:

	<p>By phone</p> <p>Call us on 0333 207 2229 or contact your Relationship Team.</p> <p>To maintain a quality service we may maintain or record phone calls for training and security purposes.</p>
---	--

Right to object to processing

In certain circumstances you can object to the processing of your personal information.

To object to the processing of your personal information for marketing or market research, please refer to the 'Changing your marketing preferences' section of this booklet.

If you object to the processing of your personal data for any other reason, it may mean we can't provide certain products and services to you.

Right to restrict processing



You can ask us to restrict processing your data, for example where:

- you're contesting the accuracy of your personal data;
- we no longer need to process your personal data, but you want us to keep it for use in legal claims; or
- you've objected to the processing by asking us to stop using your data, but you're waiting for us to tell you if we have overriding grounds which mean we're allowed to keep on using it.

If the right applies, this means with the exception of storage, your personal data can only be processed by us with your consent or for certain things such as legal claims or to exercise legal rights.

If you request that we restrict the processing of your personal data it may mean we can't provide certain products and services to you.

To request a right to object to, or restrict processing you can contact us:

	<p>By phone</p> <p>Call us on 0333 207 2229 or contact your Relationship Team.</p> <p>To maintain a quality service we may maintain or record phone calls for training and security purposes.</p>
	<p>By post</p> <p>Write to us: Santander Corporate & Commercial Banking Sunderland SR43 4GG</p>



Right to erasure (Right to be forgotten)

In the circumstances below you can ask us to delete your personal data. Where the right doesn't apply we'll let you know why we can't action your request.

This right may be applied where:

- personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- the processing was based on your consent which you withdraw (and there are no other legal grounds for processing that data);
- you exercise your right to object and there are no overriding legitimate grounds for the processing; or
- there is no lawful reason to retain personal data or if the personal data has to be erased to comply with a legal obligation.

To request a right to erasure you can contact us:



	<p>By phone</p> <p>Call us on 0333 207 2229 or contact your Relationship Team.</p> <p>To maintain a quality service we may maintain or record phone calls for training and security purposes.</p>
	<p>By post</p> <p>Write to us: Santander Corporate & Commercial Banking Sunderland SR43 4GG</p>

Right to portability

You can ask us to provide you with a copy of certain personal data in a structured, commonly used, machine-readable format. This right only applies to personal data that you've previously provided to us, we process electronically and we're processing based on your consent or to perform a contract with you. Your account must also be open in order to exercise this right.

If you request a right to portability on a joint account, and you're an account owner, trustee, registered contact or holder, you'll receive your own personal data, and any transactional data linked to that account. Other account users (i.e. beneficiary or additional member) will only receive their personal data and won't receive any transactional data. All account users will need to make a separate request for their data.

To request a right to portability you can contact us:

	<p>By phone</p> <p>Call us on 0333 207 2229 or contact your Relationship Team.</p> <p>To maintain a quality service we may maintain or record phone calls for training and security purposes.</p>
	<p>By post</p> <p>Write to us: Santander Corporate & Commercial Banking Sunderland SR43 4GG</p>

Changing your marketing preferences

You can select the types of marketing you receive with our Marketing Preference Centre which is accessible via our website and link in marketing communications.

Sharing of your personal data

If you open an account with us, your information will be kept after your account is closed. Your information may be shared across the Santander Group or associated companies, service providers or agents for administration purposes to:



- provide and run the account or service you have applied for, and develop and/or improve our products and services;
- identify and advise you by post, telephone or electronic media (including email) of products or services which our group of companies and our associated companies think may be of interest to you (for credit products this may involve releasing your details to a credit reference agency); and
- release your name, address and telephone number to market research organisations for the purpose of confidential market research surveys, carried out by post or telephone, on our behalf.

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.

The easiest and quickest way to get in touch about a complaint is by talking to our dedicated Complaints Team.

To talk to our dedicated Complaints Team you can contact us:

	By phone
	<p>Call us on 0333 207 2229 or contact your Relationship Team.</p> <p>To maintain a quality service we may maintain or record phone calls for training and security purposes.</p>
	By post <p>Write to us at the address below, providing as much detail as possible about what's gone wrong, along with your name, address, account number, phone number and a convenient time for us to call you to discuss your complaint.</p> <p>Complaints Santander Corporate & Commercial Banking Complaints Team Sunderland SR43 4GZ</p>

Our Santander Complaints Leaflet is available upon request and contains further information on our complaints process, including the handling timescales. This information is also available on [santander.co.uk](https://www.santander.co.uk).

Our Santander Corporate & Commercial Complaints Leaflet is available on [santander.co.uk/corporate](https://www.santander.co.uk/corporate).



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. You can find out more information at [financial-ombudsman.org.uk](https://www.financial-ombudsman.org.uk).

Data subject access requests

You have the right to find out what personal information, if any, is held about you. This is known as a data subject access request.

A data subject access request is not designed to deal with general queries that you may have about your account. For corporate clients it is unlikely to provide any information about the company. We want to give you the information you need without you having to make a formal request. If you'd like to find out specific information about your account, you can contact us by phone.

To make a formal data subject access request you can contact us:

	By post
	<p>Write to us at the address below, providing:</p> <ul style="list-style-type: none"> ◦ your full name and date of birth; ◦ a daytime phone number in case we need to contact you to discuss your request; ◦ your sort code and account number(s); ◦ your company name and reference number; and ◦ detail on whether your request relates to your corporate or personal relationship with us, or both. <p>If your request doesn't relate to an account, please let us know the nature of your relationship with Santander and any other relevant information.</p> <p>Santander Subject Access Requests Sunderland SR43 4FN</p>
	By phone
	<p>Call us on 0333 207 2229 or contact your Relationship Team.</p> <p>To maintain a quality service we may maintain or record phone calls for training and security purposes.</p>

Automated decision making and processing

In some instances we'll undertake automated processing and decision-making to decide which of our other products or services might be of interest to you. You have a right not to have a decision made based solely on automated processing (including profiling) that produces legal or similar effects. This doesn't apply where the processing is necessary for the performance of a contract, is authorised by law, or the person has given their consent to the processing (though they can revoke their consent thereafter).

Where you have been adversely affected by an automated decision, and/or you think we have made a mistake, or you have further information to support your case, there is an underwriting process in place. We can't guarantee to reverse a decision, but we'll always be happy to reconsider your application if you believe you have been wrongly declined.

To ask us to reconsider your application you can contact us on 0333 207 2229 or contact your Relationship Team.

Glossary of terms

Behavioural scoring

Techniques that help organisations decide whether or not to grant credit to customers.

Beneficiary bank

A beneficiary bank is the receiving bank where you have your account.

Binding Corporate Rules

Personal data protection policies which are adhered to by a controller or processor established in the United Kingdom 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.

Biometric data

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of an individual, which allows or confirms the unique identification of that individual, such as facial images or things like fingerprints.

CHAPS

Clearing House Automated Payment System.

Data Controller

The natural or legal person, public authority, agency or other body which alone or jointly with others, determines the purposes and means of the processing of personal data.

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.

Special categories of personal data

The special categories of personal data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data or data concerning an individual's sex life or sexual orientation, and the processing of genetic data or biometric data for the purpose of uniquely identifying an individual.

