Using my personal data

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

Santander International

Contents

The Data Protection Statement

Introduction

My personal data is data which by itself, or with other data available to you, can be used to identify me. You are Santander International, which is the trading name of Santander Financial Services plc, Jersey Branch and Santander Financial Services plc, Isle of Man Branch, the data controller. This data protection statement sets out how you will use my personal data.

The types of personal data you collect and use

Whether or not I become a customer, you will use my personal data for the reasons set out below and if I become a customer you will use it to manage the account, policy or service I have applied for. You will collect most of this directly during the application process. The sources of personal data collected indirectly are mentioned in this statement. The personal data you use may be about me as a personal or business customer and may include:

- Full name, personal details including contact information (e.g. home address and address history, email, home and mobile telephone numbers);
- Date of birth;
- Financial details (e.g. salary and details of other income, and details of accounts held with other providers);
- Records of products and services I have obtained or applied for, how I use them and the relevant technology used to access or manage them (e.g. IP address, MAC address);
- Information from credit reference or fraud prevention agencies, electoral roll, court records of debt judgements and bankruptcies and other publicly available sources as well as information on any financial associates I may have;
- Family, lifestyle or social circumstances if relevant to the product or service (e.g. the number of dependants I have);
- Education and employment details/employment status for credit and fraud prevention purposes; and
- Personal data about other named applicants. I must have their authority to provide their personal data to you and share this data protection statement with them beforehand together with details of what I have agreed on their behalf.

Providing my personal data

You will tell me if providing some personal data is optional, including if you ask for my consent to process it. In all other cases, I must provide my personal data so you can process my application (unless I am a customer and you already hold my details).

Monitoring of communications

Subject to applicable laws in the Isle of Man and/or Jersey, you will monitor and record my calls; emails; social media messages and other communications related to my dealings with you. You will do this for regulatory compliance, self-regulatory practices, crime prevention and detection, to protect the security of your communications systems and procedures; to check for obscene or profane content; for quality control and staff training; and when you need to see a record of what's been said. You may also monitor activities on my account where necessary for these reasons and this is justified by your legitimate interests or your legal obligations.

Using my personal data: the legal basis and purposes

You will process my personal data:

1. As necessary to perform your contract with me for the relevant account, policy or service:
    a) To take steps at my request prior to entering into it;
    b) To decide whether to enter into it;
    c) To manage and perform that contract;
    d) To update your records; and
    e) To trace my whereabouts to contact me about my account and recovering debt.
2. As necessary for your own legitimate interests or those of other persons and organisations, e.g.:
    a) For good governance, accounting, and managing and auditing your business operations;
    b) To search at credit reference agencies if I am over 18 and apply for credit;
    c) To monitor emails, calls, other communications, and activities on my account;

d) For market research, analysis and developing statistics; and

e) To send me marketing communications, including automated decision making relating to this.

3. As necessary to comply with a legal obligation, e.g.:

a) When I exercise my rights under data protection law and make requests;

b) For compliance with legal and regulatory requirements and related disclosures;

c) For establishment and defence of legal rights;

d) For activities relating to the prevention, detection and investigation of crime;

e) To verify my identity, make credit, fraud prevention and anti-money laundering checks; and

f) To monitor emails, calls, other communications, and activities on my account.

4. Based on my consent, e.g.:

a) When I request you to disclose my personal data to other people or organisations such as a company handling a claim on my behalf, or otherwise agree to disclosures; and

b) To send me marketing communications where you've asked for my consent to do so.

You do not currently process any special categories of personal data about me (e.g. my racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning my health, sex life or sexual orientation) however, if this changes in future you will request my consent to do so.

I am free at any time to change my mind and withdraw my consent. The consequences might be that You may be unable to provide me with certain products or services and this may result in the closure of the account.

Sharing of my personal data

Subject to applicable data protection law in the Isle of Man and/or Jersey you may share my personal data with:

- The Santander group of companies and associated companies in which you have shareholdings and employees, officers, agents or professional advisors of these companies;
- Sub-contractors and other persons who help you provide your products and services;
- Companies and other persons providing services to you;
- Your legal and other professional advisors, including your auditors;
- Fraud prevention agencies, credit reference agencies, and debt collection agencies when you open my account and periodically during my account or service management;
- Other organisations who use shared databases for income verification and affordability checks and to manage/collect arrears;
- Government bodies and agencies in the Isle of Man; Jersey; and overseas (e.g. the Isle of Man or Jersey Tax Authorities who may in turn share it with relevant overseas tax authorities and with regulators e.g. the Isle of Man Financial Services Authority, the Jersey Financial Services Commission, the Isle of Man Information Commissioner; and the Office of the Information Commissioner (Jersey));
- Courts, to comply with legal requirements, and for the administration of justice;
- Other parties where necessary in an emergency or to otherwise protect my vital interests;
- Other parties where necessary to protect the security or integrity of your business operations;
- Other parties connected with my account e.g. guarantors and other people named on the application including joint account holders will see my transactions;
- Other parties when you restructure or sell your business or its assets or have a merger or re-organisation;
- Market research organisations who help to improve your products or services;
- Payment systems (e.g. Visa) if you issue cards linked to my account who may transfer my personal data to others as necessary to operate my account and for regulatory purposes, to process transactions, resolve disputes and for statistical purposes, including sending my personal data overseas; and
- Anyone else where you have my consent or as required by law.

You require all third parties to respect the security of my personal data and treat it in accordance with the law. You do not allow your third party service providers to use my personal data for their own purposes and only permit them to process my personal data for specified purposes and in accordance with your instructions.

International transfers

My personal data may be transferred outside Jersey; Isle of Man; and the European Economic Area. 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.

Identity verification and fraud prevention checks

The personal data you've collected from me at application or at any stage will be shared with fraud prevention agencies who will use it to prevent fraud and money-laundering and to verify my identity. If fraud is detected, I could be refused certain services, finance or employment in future. You may also search and use your internal records for these purposes. You may also hold all the information I give to you (i.e. name, address, date of birth, nationality) to undertake periodic due diligence checks which banks are required to undertake to comply with Isle of Man and Jersey legislation.

Credit reference checks

If I have applied for a credit product then in order to process my application, you will perform credit and identity checks on me with one or more credit reference agencies. To do this you'll supply my personal data to the credit reference agencies and they will give you information about me.

When you carry out a search at the credit reference agencies they will place a footprint on my credit file. A credit search may either be:

a) a quotation search where a soft footprint is left. This has no effect on my credit score, and lenders are unable to see this; or

b) a hard footprint where I have agreed/requested Santander International to proceed with my application for credit. This footprint will be viewable by other lenders and may affect my ability to get credit elsewhere. (A credit search is not carried out if I am under 18)

You will also continue to exchange information about me with credit reference agencies while I have a relationship with you. The credit reference agencies may in turn share my personal information with other organisations. Details about my application (whether or not it is successful) will be recorded and you will give details of my accounts and how I manage them to credit reference agencies.

If I do not repay any debt in full or on time, they will record the outstanding debt and supply this information to others performing similar checks, to trace my whereabouts and to recover debts that I owe. Records remain on the files of credit reference agencies for 6 years after my account is closed, whether settled by me or defaulted. A financial association link between joint applicants will be created at the credit reference agencies. This will link our financial records and be taken into account in all future applications by either or both of us until either of us apply for a notice of disassociation with the 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 on page 12, or 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

My marketing preferences and related searches

You will use my home address, phone numbers, email address and social media (e.g. Facebook and message facilities in other platforms) to contact me according to my preferences. I can change my preferences or unsubscribe at any time by contacting you. If I am over 18, you may search the files at credit reference agencies before sending marketing communications or doing marketing in-branch to me about credit. The credit reference agencies do not record this particular search or show it to other lenders and it won't affect my credit rating. You do this as part of your responsible lending obligations, which is within your legitimate interests.

I understand that from time to time you would like to contact me with details of other products and services you think may interest me or to get my opinion on how you are doing. I confirm that I have been asked about my marketing preferences as part of my application and I understand that if I have previously told you that I don't want information on other products and services or to be included in market research, you'll continue to respect my wishes. I understand I can choose to stop receiving information at any time by contacting you.

For joint account customers, if your marketing preferences selection are different we may decide **not** to contact you using that preference, if your individual marketing preferences are not the same.

Automated decision making and processing

Automated decision making involves processing my personal data without human intervention to evaluate my personal situation such as my economic position, personal preferences, interests or behaviour, for instance in relation to transactions on my accounts, my payments to other providers, and triggers and events such as account opening anniversaries and maturity dates. You may do this to decide what marketing communications are suitable for me, to analyse statistics and assess lending and insurance risks. All this activity is on the basis of your legitimate interests, to protect your business, and to develop and improve your products and services, except as follows; when you 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 me or to take steps to enter into that contract.

Criteria used to determine retention periods (whether or not I become a customer)

The following criteria is used to determine data retention periods for my personal data:

- Retention in case of queries. You will retain my personal data as long as necessary to deal with my queries (e.g. if my application is unsuccessful);
- Retention in case of claims. You will retain my personal data for as long as I might legally bring claims against you; and
- Retention in accordance with legal and regulatory requirements. You will retain my personal data after my account, policy or service has been closed or has otherwise come to an end based on your legal and regulatory requirements.

My rights under applicable data protection law

My rights are as follows:

- The right to be informed about your processing of my personal data;
- The right to have my personal data corrected if it is inaccurate and to have incomplete personal data completed;
- The right to object to processing of my personal data;
- The right to restrict processing of my personal data;
- The right to have my personal data erased (the 'right to be forgotten');
- The right to request access to my personal data and information about how you process it;
- The right to move, copy or transfer my personal data ('data portability'); and
- Rights in relation to automated decision making including profiling.

I understand that I will not have to pay a fee to access my personal data (or to exercise any of the other rights). However, you may charge a reasonable fee if my request is clearly unfounded, repetitive or excessive. Alternatively, you may refuse to comply with my request in these circumstances.

Depending on where my account is held, I have the right to complain to the Isle of Man Information Commissioner's Office www.inforights.im/ or the Office of the Information Commissioner (Jersey) www.oicjersey.org. Both have enforcement powers and can investigate compliance with data protection law.

For more details on all the above I can contact your Data Protection Officer.

Data anonymisation and aggregation

My personal data may be converted into statistical or aggregated data which cannot be used to identify me, then used to produce statistical research and reports. This aggregated data may be shared and used in all the ways described above.

Updating our Data Protection Statement

We may update the data protection statement from time to time. When we change the data protection statement in a material way, this will be communicated to you together with the updated data protection statement.

Business Changes

If we or the Santander group undergoes a group reorganisation or is sold to a third party, your personal information provided to us may be transferred to that reorganised entity or third party and used for the purposes highlighted in this data protection statement.

The Data Protection Statement explained

Introduction

This section sets out who the Data Controller is and provides contact details for the Data Protection Officer ('DPO').

In the Data Protection Statement 'we' or 'Santander International' means Santander Financial Services plc, Jersey Branch and Santander Financial Services plc, Isle of Man Branch. In legal terms Santander International is designated as the Data Controller because it is the entity that (either alone or jointly with others) determines the purposes and means of the processing of your personal data.

If you have any questions about how your personal data is used, or the information included in this booklet, our DPO can be contacted at Santander International, 13-15 Charing Cross, St Helier, Jersey JE2 3RP, Channel Islands.

The types of personal data we collect and use

The sort of personal data we collect and use will vary depending on the products or services you require or have, and your preferred relationship with us.

Whether providing your personal data is required by law or contract or not

This section states that you will be told whether the provision of your personal data is optional or mandatory.

If the provision of the data is mandatory and we don't already hold it then you will need to provide the information so that we can process your application, service and maintain your account.

Monitoring of communications

This section explains why we may monitor your on-going communications with us.

This includes us monitoring our communications with you so that we comply with regulatory rules, or our own internal processes and protocols:

- 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 have said to you/what you have said to us. For example, where we are required by the Isle of Man Financial Services Authority ('IOMFSA') or the Jersey Financial Services Commission ('JFSC') 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 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 are subject.

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 the service being provided.

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.

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, 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. Please note: The bank(s) we may share your data with may be located outside of the European Economic Area ('EEA'), and therefore may not be subject to the same data privacy legal obligations as banks within the EEA.

Complying with established legal obligations is another reason for us to share your personal data. For example if you require us to transfer funds via CHAPS or internationally, via SWIFT 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 EEA. This information may include your full name, address, date of birth and account number – and by making your payment instructions to us, you consent to us sharing personal information to overseas authorities and beneficiary bank(s) as appropriate.

Consent for processing of special categories of personal data, at your request, must be explicit. For example:

(i) If we require a copy of your passport (as a new customer) and if that reveals your racial or ethnic origin data, by providing a copy you will be explicitly consenting to us seeing your racial or ethnic origin in this way.

(ii) If you volunteer data concerning your health when we ask you about the conduct of your account you will be explicitly consenting to us processing this personal data in connection with your account.

Under Data Protection legislation you can withdraw your consent at any time. If you do this, and if there is 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.

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.

Subject to applicable data protection law in the Isle of Man and/or Jersey you may share my personal data with the Santander group of companies, as defined in the Glossary of Terms under the heading of Group Companies, and associated companies in which you have shareholdings and employees, officers, agents or professional advisors of these companies, some of whom may be in other countries. As outlined in our General Terms and Conditions we will ensure your information is used in line with our own strict confidentiality policies and as required under data protection legislation in the relevant jurisdiction.

International transfers

This section explains that where we transfer your personal data outside of the Isle of Man, Jersey and the 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 DPO.

(ii) The US Privacy Shield and details are available here: privacyshield.gov/welcome or from our 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 DPO.

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.

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.

Your marketing preferences and related searches

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.

You can provide your specific marketing preferences as part of your application. Equally you can contact us at any time to provide and/or update those preferences.

Automated decision making and processing

This section explains what automated decision making is, and the circumstances when it may take place.

We may automatically process your personal data, without human intervention, to evaluate certain personal aspects about you (known as profiling).

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 data. 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.

We may use your personal data to assess lending risk. If we conduct automated decision making including profiling activity to assess lending 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.

In some instances we may use automated processing and decision making, where relevant, to decide which of our other products or services might be suitable for you. We will 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 may 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.

We may use the information from this activity to:

(i) Decide which other products and/or services from us or the Santander Group of companies, 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 the Santander Group of companies. This means that automated decisions and processing can help to determine what marketing communications you receive, and what marketing happens face-to-face when you visit us in-branch (this is what we mean in our Data Protection Statement when we refer to 'marketing in-branch').

(ii) Send marketing communications to you and to conduct marketing in-branch to you.

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. 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.

Where profiling is based on legitimate interests you have the right to object to that processing.

Criteria used to determine retention periods

This section within the Data Protection Statement explains the criteria we use when deciding how long personal data needs to be retained.

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 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 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 that is lawful and permitted under Data Protection law, for instance where the personal data has to be retained to comply with other 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 we process it. This is more commonly known as submitting a 'data subject access request'. This must be done in writing. 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 (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.
- To complain to the relevant Information Commissioner, the independent bodies empowered to investigate whether we are complying with the Data Protection law, based on the branch where your account is held. You can do this if you consider that we have infringed the legislation in any way. You can visit their websites for more information.

Isle of Man	Jersey
www.inforights.im	www.jerseyoic.org

If you seek to exercise any of your rights against us we will 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.

Data anonymisation and aggregation

This section explains that your personal data may be turned into statistical or aggregated data, data that can no longer identify you.

Your personal data may be converted ('anonymised') into statistical or aggregated data in such a way as to ensure that you are not identified or identifiable from it. Aggregated data can't, by definition, be linked back to you as an individual. This data might be used to conduct research and analysis, including to prepare statistical research and reports. This data may be shared in several ways, including with the Santander Group companies, and for the same reasons as set out in the Data Protection Statement.

Updating our Data Protection Statement

We may update the data protection statement from time to time. When we change the data protection statement in a material way, this will be communicated to you together with the updated data protection statement.

Business Changes

If we or the Santander group undergoes a group reorganisation or is sold to a third party, your personal information provided to us may be transferred to that reorganised entity or third party and used for the purposes highlighted in this data protection statement.

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 have provided us with, details we have collected from you directly, and/or information we have 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 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.

Fraud prevention 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.

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 that of known fraudsters, or money launderers, 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 have 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

Whenever fraud prevention agencies transfer your personal data outside of the 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

Credit reference agencies explained

When we process your application, we will perform standard credit and identity checks on you with one or more credit reference agencies. Where we provide banking services for you we may also conduct periodic searches at the credit reference agencies to manage your account.

In doing this we will supply your personal information to the credit reference agencies and they will give us information about you. This, if applicable, will include information from any credit application you may make, 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 electoral registers), and shared credit, financial, and fraud prevention information.

We will use this information to:

- assess your creditworthiness, and whether you can afford to repay the financial product in question;
- verify the accuracy of the data you have provided to us;
- prevent criminal activity, fraud and money laundering;
- manage your account(s);
- trace and recover debts; and
- ensure any offers provided to you are appropriate to your circumstances.

We will continue to exchange information about you with the credit reference agencies while you have a relationship with us. We will also inform credit reference agencies about your settled accounts. If you borrow and do not repay in full and on time, credit reference agencies will record the outstanding debt. 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, civil partner or any other person you wish to hold an account with in joint names, we will 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 please contact:

Trans Union

Consumer Services Team, PO Box 491
Leeds
West Yorkshire
LS3 1WZ
Telephone: 0330 024 7574
Website: transunion.co.uk/crain

Equifax

Equifax Ltd
Customer Service Centre, PO Box 10036
Leicester LE3 4FS
Telephone: 0333 321 4043 or 0800 014 2955
Website: equifax.co.uk/crain

Experian

Experian
Customer Support Centre, PO Box 9000
Nottingham
NG80 7WF
Telephone: 0344 481 0800 or 0800 013 8888
Website: experian.co.uk/crain

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.

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 please contact us using the details on page 14 of this booklet.

Marketing and market research opt-out

If you'd prefer not to continue to receive up-to-date information on our products and services, or to be included in market research, you can indicate this by updating your marketing preferences at any time.

To opt-out of marketing and market research please contact us using the details on page 14 of this booklet.

E-mail opt-out

If you have previously opted to receive marketing emails and don't want to in future, please use the unsubscribe link within the email and we will remove you from all future campaigns.

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 and SMS) 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).

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 calling us (contact details are on page 14 of this booklet).

Our Complaints Leaflet is available upon request and contains further information on our complaints process, including the handling timescales. This information is also available on our website at https://www.santanderinternational.co.uk/contact-us/complaints

You may also be able to refer your complaint to the relevant 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:

Isle of Man:

www.gov.im/about-the-government/statutory-boards/isle-of-man-office-of-fair-trading/financial-services-ombudsman-scheme/

Jersey:

www.ci-fo.org/

Data subject access requests

You have the right to find out what 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. We therefore aim to provide you with the information you require without you having to make a formal request. If you would like to find out specific information about your account, you can contact us by phone or in branch.

To make a formal data subject access request please contact us using the details on page 14 of this booklet.

Automated decision making and processing

In some instances we may 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 will always be happy to reconsider your application if you believe you have been wrongly declined.

To ask us to reconsider your application, please contact us.

Our contact details – Isle of Man branch

Visit us at Santander Work Cafe, Market Hall, North Quay, Douglas, Isle of Man IM1 2BQ or write to us at Santander International, PO Box 123, 19-21 Prospect Hill, Douglas, Isle of Man IM99 1ZZ, British Isles

08000 84 28 88 – from a UK landline or mobile, or+44 (0)1624 641 888 – if calling from overseas

Monday to Friday 9am to 5pm (UK time), except Wednesdays when we open at 9.30am.

info@santanderinternational.co.uk

santanderinternational.co.uk

Our contact details – Jersey branch

Santander International, 13-15 Charing Cross, St Helier, Jersey JE2 3RP, Channel Islands

08000 84 28 88 – from a UK landline or mobile, or +44 (0)1534 885 000 – if calling from overseas

Monday to Friday 9am to 5pm (UK time), except Wednesdays when we open at 9.30am.

info@santanderinternational.co.uk

santanderinternational.co.uk

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 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.

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.

Cifas

Cifas is a not-for-profit fraud prevention membership organisation. Cifas is the UK's leading fraud prevention service, managing the largest confirmed fraud database in the country. Members are organisations from all sectors, sharing their data across those sectors to reduce instances of fraud and financial crime.

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. Where the purposes and means of such processing are determined by Crown Dependency or European Union Member State law, the controller or the specific criteria for its nomination may be provided for by Crown Dependency or EU Member State law.

Data Protection Officer (DPO)
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.

Group companies
The Santander group of companies includes but is not limited to Banco Santander S.A., SCF Madrid, S.A.; Santander UK Group Holdings plc, Santander UK plc, Santander Financial Services plc, Santander UK Santander Consumer (UK) plc trading as Santander Consumer Finance; Santander Insurance Services UK Ltd.

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.

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.

To find out more

08000 84 28 88 if calling from a UK landline or mobile,
or +44 (0)1624 641 888 if calling from overseas.
Monday to Friday 9am to 5pm (UK time), except Wednesdays when we open at 9.30am.

santanderinternational.co.uk

info@santanderinternational.co.uk

Visit us at:

Santander Work Café
Market Hall, North Quay
Douglas, Isle of Man IM1 2BQ,
British Isles
or
Santander Work Café
13-15 Charing Cross,
St Helier, Jersey JE2 3RP,
Channel Islands

Write to us at:

Santander International
PO Box 123, 19-21 Prospect Hill,
Douglas, Isle of Man IM99 1ZZ,
British Isles

Santander International is able to provide this document in large print, Braille and audio CD. If you would like to receive this document in one of these formats, please contact us.

ABIN 0511 DEC23 L