IMPORTANT INFORMATION
Please read and keep for future reference

Using my personal data

How we use your personal data

When you applied for an account with cahoot you will have 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

1. The 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 cahoot which is a division of Santander UK plc 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 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 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. For instance, biometric data will be captured if you register your fingerprints for Mobile Banking, or your voice recordings for voice activated banking.
Whether providing your personal data is required by law or contract or not	This section states that you'll 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'll need to provide the information so that we can process your application or service.
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 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 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 what we're trying to achieve. 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, 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.

Data Protection Statement section	Explanation
Using your personal data: the legal basis and purposes (continued)	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. 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. 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 and Commercial, a brand name of Santander UK plc (which also uses the brand name Santander Corporate and Investment Banking) and of Santander Asset Finance plc; Santander Insurance Services UK Ltd and Asto Digital Limited.
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.html** or from our Data Protection Officer (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'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.

Data Protection Statement section	Explanation
Automated decision making and processing (continued)	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. The personalised price would be presented to you in marketing communications and during contacts with cahoot that might be suitable. 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. We'll use the information from this activity to: (i) 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. (ii) Send marketing communications 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, 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. 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 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 your account is open and 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.

Data Protection Statement section	Explanation
Your rights under applicable Data Protection law (continued)	■ 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. 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.
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.

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
- Proximity checking
- 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
- Vehicle details

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, 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 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

Whenever 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
Website: **www.cifas.org.uk/fpn**

The Compliance Officer
National Hunter
PO Box 4744
Stone
Staffordshire
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. Credit reference agencies explained

This section is the wording provided by the credit reference agencies, and sets out how your personal data may be used.

CREDIT REFERENCE AGENCY INFORMATION NOTICE (CRAIN)

Version: 1 – Adopted: 23 October 2017

NOTE: The information in this document will be effective from the Adopted Date set out above, except for the information in Sections 9, (data portability right), 11 and 12. These Sections provide information on new rights that will only come into effect from the 25 May 2018, which is the effective date of the General Data Protection Regulation (or the GDPR).

This document describes how the three main credit reference agencies TransUnion, Equifax and Experian, (also called "credit reference agencies" or "CRAs" in this document) each use and share personal data (also called 'bureau data') they receive about you and/or your business that is part of or derived from or used in credit activity.

Please note: you shouldn't think of this document as a complete record of all the personal data each CRA may hold and process, as each has a number of different business functions running through it. To find out more about each CRA's other businesses, services and personal data processing, go to the website links provided at Section 14 below.

This document answers these questions:

1. Who are the credit reference agencies and how can I contact them?
2. What do credit reference agencies use personal data for?
3. What are the credit reference agencies' legal grounds for handling personal data?
4. What kinds of personal data do credit reference agencies use, and where do they get it?
5. Who do credit reference agencies share personal data with?
6. Where is personal data stored and sent?
7. How long is personal data kept for?
8. Do the credit reference agencies make decisions about me or profile me?
9. What can I do if I want to see the personal data held about me? Do I have a 'data portability' right in connection with my bureau data?
10. What can I do if my personal data is wrong?
11. Can I object to the use of my personal data and have it deleted?
12. Can I restrict what the credit reference agencies do with my personal data?
13. Who can I complain to if I'm unhappy about the use of my personal data?
14. Where can I find out more?

You have the right to object to credit reference agencies using your personal data. Please see Section 11 to find out more.

1. Who are the credit reference agencies and how can I contact them?

There are three main credit reference agencies in the UK who deal with people's personal data.

Each is regulated by the Financial Conduct Authority ("FCA") and authorised to conduct business as a credit reference agency.

Credit reference agency	Contact details	
TransUnion Limited		**Post** TransUnion Information Group Limited, One Park Lane, Leeds, West Yorkshire LS3 1EP.
		Web address **https://www.transunion.co.uk/consumer-solutions/contact-us#**
		Email consumer@transunion.co.uk
		Phone 0330 024 7574
Equifax Limited		**Post** Equifax Ltd, Customer Service Centre PO Box 10036, Leicester, LE3 4FS.
		Web address **https://www.equifax.co.uk/Contact-us/Contact_Us_Personal_Solutions.html**
		Email www.equifax.co.uk/ask
		Phone 0333 321 4043 or 0800 014 2955
Experian Limited		**Post** Experian, PO BOX 9000, Nottingham, NG80 7WF.
		Web address **http://www.experian.co.uk/consumer/contact-us/index.html**
		Email consumer.helpservice@uk.experian.com
		Phone 0344 481 0800 or 0800 013 8888

2. What do credit reference agencies use personal data for?

(a) Credit reference agency processing

Credit reference agencies receive personal data about you that's part of, derived from or used in credit activity. Different lenders and creditors will use different CRA services, and may not use all the services described here, so we recommend you also check your lender and creditor's privacy policy(s) as well as this document.

Credit reporting and affordability checks

Each CRA uses the data it gathers to provide credit reporting services to its clients.

Organisations use credit reporting services to see the financial position of people and businesses. For example, a lender or creditor may check with a credit reference agency when an individual or business applies for credit and the lender or creditor needs to make a credit decision taking into account that person or business's credit history.

Affordability checks help organisations understand whether people applying for credit or financial products (like loans) are likely to afford the repayments.

These activities help promote responsible lending, prevent people and businesses from getting into more debt than they can afford, and reduce the amount of unrecoverable debt and insolvencies.

Verifying data like identity, age and residence, and preventing and detecting criminal activity, fraud and money laundering

The CRAs also use bureau data to provide verification, crime prevention and detection services to their clients, as well as fraud and anti-money-laundering services. For example:

- When a person applies to an organisation for a product or service, the organisation might ask them to answer questions about themselves, and then check the answers against the data held by the CRAs to see if they're correct. This helps confirm the person they are dealing with is not trying to commit identity theft or any other kind of fraud.
- Where some products and services are only available to people of a certain age, organisations can check whether the person they're dealing with is eligible by searching the CRAs databases.
- If a person applies for credit the lender or creditor might check the personal data that person gives them against the personal data held by CRAs to try and prevent fraud.
- Government and quasi-government bodies can use data held by CRAs to check whether people are entitled to certain benefits and to help recover unpaid taxes, overpaid benefits and similar debts.

Account management

CRAs supply information including personal data to their clients for account management, which is the ongoing maintenance of the client organisation's relationship with its customers.

This could include activities designed to support:

- data accuracy (such as data cleansing - where bureau data can be used to clean or update lender data. This might involve checks that data is in the right format or fields, or to correct spelling errors);
- clients' ongoing account management activities. (For example, data sharing with lenders and creditors so clients can make decisions relating to credit limit adjustments, transaction authorisations, and to identify and manage the accounts of customers at risk, in early stress, in arrears, or going through a debt collection process, or to confirm that assets are connected to the right person).

Tracing and debt recovery

CRAs provide services that allow organisations to use bureau data to trace people who've moved. Each CRA also offers a service that allows people to be reunited with assets (like an old dormant savings account they've lost contact with)

CRAs may also use personal data to support debt recovery and debtor tracing. An example of a tracing activity could be when a person owes money and moves house without telling the creditor where they've gone. The creditor may need help finding that person to claim back what they're owed. CRAs help find missing debtors by providing creditors with updated addresses and contact details.

Screening

CRAs can use some personal data to screen people out of marketing lists. For example, where a person's financial history suggests they're unlikely to be accepted for or afford a particular product, the relevant organisation can use that data to opt out of sending them information about that product. This helps stop people receiving irrelevant marketing, and saves organisations the costs of inappropriate marketing and unsuccessful applications.

The data isn't used to identify, select and send marketing materials to potential new customers.

Statistical analysis, analytics and profiling

CRAs can use and allow the use of personal data for statistical analysis and analytics purposes, for example, to create scorecards, models and variables in connection with the assessment of credit, fraud, risk or to verify identities, to monitor and predict market trends, to allow use by lenders for refining lending and fraud strategies, and for analysis such as loss forecasting.

Database activities

CRAs carry out certain processing activities internally which support databases effectiveness and efficiencies. For example:

- Data loading: where data supplied to the CRAs is checked for integrity, validity, consistency, quality and age help make sure it's fit for purpose. These checks pick up things like irregular dates of birth, names, addresses, account start and default dates, and gaps in status history.
- Data matching: where data supplied to the CRAs is matched to their existing databases to help make sure it's assigned to the right person, even when there are discrepancies like spelling mistakes or different versions of a person's name. CRAs use the personal data people give lenders together with data from other sources to create and confirm identities, which they use to underpin the services they provide.
- Data linking: as CRAs compile data into their databases, they create links between different pieces of data. For example, people who appear financially associated with each other may be linked together, and addresses where someone has previously lived can be linked to each other and to that person's current address.
- Systems and product testing: data may be used to help support the development and testing of new products and technologies.

Each CRA has its own processes and standards for data loading, data matching and other database processing activities.

Other uses with your permission

From time to time CRAs may use the personal data they hold or receive about you for other purposes where you've given your consent.

Uses as required by or permitted by law

Your personal data may also be used for other purposes where required or permitted by law.

Other activities

Each credit reference agency also has other lines of business not described in this document. For example, each offers its own marketing services and direct-to-consumer services. Each CRA will provide separate information as appropriate for any services that fall outside of scope of this document.

(b) What is a fraud prevention agency?

A Fraud Prevention Agency (FPA) collects, maintains and shares, data on known and suspected fraudulent activity. All three credit reference agencies also act as FPAs.

(c) Fraud prevention agency processing

How data may be used by fraud prevention agencies:

FPAs may supply the data received from lenders and creditors about you, your financial associates and your business (if you have one) to other organisations (please see Section 5 for more information on these organisations). This may be used by them and the CRAs to:

Prevent crime, fraud and money laundering by, for example;

- checking details provided on applications for credit and credit related or other products and services
- Managing credit and credit related accounts or products or services
- Cross-checking details provided on proposals and claims for all types of insurance
- Checking details on applications for jobs or as part of employment
- Verify your identity if you or your financial associate applies for facilities including all types of insurance proposals and claims
- Trace your whereabouts and recover debts that you owe
- Conduct other checks to prevent or detect fraud
- Undertake statistical analysis and system testing
- Your personal data may also be used for other purposes where you've given consent or where required or permitted by law

3. What are the credit reference agencies' legal grounds for handling personal data?

Legitimate interests

The UK's data protection law allows the use of personal data where its purpose is legitimate and isn't outweighed by the interests, fundamental rights or freedoms of data subjects.

The law calls this the Legitimate Interests condition for personal data processing.

The Legitimate Interests being pursued here are:

Interest	Explanation
Promoting responsible lending and helping to prevent over-indebtedness.	Responsible lending means that lenders only sell products that are affordable and suitable for the borrowers' circumstances. CRAs help ensure this by sharing personal data about potential borrowers, their financial associates where applicable, and their financial history. A comprehensive range of measures exists in the UK to underpin the balance so the legitimate interests aren't outweighed by the interests, fundamental rights and freedoms of data subjects. Further explanation about this balance is set out below.
Helping prevent and detect crime and fraud and anti-money laundering services and verify identity	CRAs provide identity, fraud and anti-money laundering services to help clients meet legal and regulatory obligations, and to the benefit of individuals to support identity verification and support of detection/ prevention of fraud and money-laundering.
Supporting tracing and collections	CRAs provide services that support tracing and collections where there is a legitimate interest in the client conducting activity to find its customer and to recover the debt, or to reunite, or confirm an asset is connected with, the right person.
Complying with and supporting compliance with legal and regulatory requirements	CRAs have to comply with various legal and regulatory requirements. CRA services also help other organisations comply with their own legal and regulatory obligations. One example, many kinds of financial services are regulated by the Financial Conduct Authority or the Prudential Regulation Authority, who impose obligations to check that financial products are suitable for the people they are being sold to. The credit reference agencies provide data to help with those checks.

The CRAs use of this personal data is subject to an extensive framework of safeguards that help make sure that people's rights are protected. These include the information given to people about how their personal data will be used and how they can exercise their rights to obtain their personal data, have it corrected or restricted, object to it being processed, and complain if they're dissatisfied. These safeguards help sustain a fair and appropriate balance so the CRAs' activities don't override the interests, fundamental rights and freedoms of data subjects.

4. What kinds of personal data do credit reference agencies use, and where do they get it?

Each credit reference agency obtains and uses information from different sources, so they often hold different information and personal data from each other. However, most of the personal data they do hold falls into the categories outlined below from the sources described.

Information type	Description	Source
Identifiers	CRAs hold personal data that can be used to identify people, like their name, date of birth, and current and previous addresses. They may also hold business data.	This personal data is included with all the other data sources. For example, names, addresses and dates of birth are attached to financial account data so it can be matched and associated with all the other data the CRA holds about the relevant person. Data about UK postal addresses is also obtained from sources like Royal Mail. CRAs also obtain copies of the electoral register containing the names and addresses of registered voters from local authorities across the UK in accordance with specific legislation. CRAs also have access to public data sources on people and businesses, including from the Insolvency Service, Companies House and commercial business directories.
Lender provided and creditor provided data	CRAs receive information that includes personal data from credit applications and about the financial accounts that people hold from the organisations that maintain those accounts. This includes personal data about bank accounts, credit card accounts, mortgage accounts and other agreements that involve a credit arrangement like utilities and communications contracts (including mobile and internet). The collected data includes the name of the organisation the account is held with, the date it was opened, the account number, the amount of debt outstanding (if any), any credit limits and the repayment history on the account, including late and missing payments. CRAs may also receive data about financial accounts like current accounts, credit cards or loans and may receive payments information that businesses hold from the organisations who maintain those accounts.	Banks, building societies, lenders and other financial services providers supply data including personal data about peoples' financial accounts and repayments. Other credit providers, such as hire purchase companies, utilities companies, mobile phone networks, retail and mail order, and insurance companies also provide this data when they agree credit facilities with their customers. These organisations may also provide Cifas markers when they suspect fraud. You can find out more about Cifas markers in the Fraud prevention indicators section below.
Court judgments, decrees and administration orders	CRAs obtain data about court judgments that have been issued against people. This may include, for example, the name of the court, the nature of the judgment, how much money was owed, and whether the judgment has been satisfied.	The government makes court judgments and other decrees and orders are made publicly available through statutory public registers. These are maintained by Registry Trust Limited, which also supplies the data on the registers to the CRAs.
Bankruptcies, Individual Voluntary Arrangement (IVAs), debt relief orders and similar events	CRAs obtain data about insolvency related events that happen to people and may also obtain this type of data about businesses. This includes data about bankruptcies, IVAs and debt relief orders, and in Scotland it includes sequestrations, trust deeds and debt arrangement schemes. This data includes the start and end dates of the relevant insolvency or arrangement.	CRAs obtain this data from The Insolvency Service, the Accountant in Bankruptcy, The Stationary Office and Northern Ireland's Department for the Economy – Insolvency Service, the London, Belfast and Edinburgh Gazettes. Business bankruptcies data are obtained from the London, Belfast and Edinburgh Gazettes.
Fraud prevention indicators	The CRAs are all Fraud Prevention Agencies (FPAs) and members of Cifas (www.cifas.org.uk), an organisation that collects and shares data about suspected fraud. When an organisation believes it's detected fraud or an attempted fraud, it may put a Cifas marker on the relevant person's credit file to warn other lenders this identity may have been used fraudulently. This helps to prevent any further fraud and protect innocent consumers.	These fraud indicators are shared among Cifas members through the database held by Cifas.

Information type	Description	Source
Gone Away Information Network indicators	Some CRAs are members of the Gone Away Information Network (GAIN), a database of people with overdue outstanding debts who've moved without giving their lender a forwarding address. Data from GAIN, including the persons' old addresses and any known new addresses, may be recorded on the relevant credit file.	CRAs obtain GAIN data from lenders, and additional address data is obtained from Royal Mail.
Search footprints	When an organisation uses a CRA to make enquiries about a particular person, the CRA keeps a record of that enquiry which appears on the person's credit file. This includes the name of the organisation, the date, and the reason they gave for making the enquiry.	CRAs generate search footprints when enquiries are made about a particular person. The organisation making the enquiry provides some of the data in the footprint (such as the reason for the enquiry).
Scores and ratings	CRAs may use the data they receive to produce scores and ratings including credit, affordability, risk, fraud and identity, screening, collections and insolvency scores about people and businesses and credit ratings about people. Organisations that obtain data from CRAs may use it together with other data to provide their own scores and ratings. Credit scores and credit ratings are produced from data like the person's credit commitments, whether they have made repayments on time, whether they've any history of insolvencies or court judgments, and how long they've lived at their current address. Each CRA has its own way of calculating credit scores, and most lenders have their own scoring systems too.	The CRAs produce their scores and ratings using the data available to them. Similarly, other organisations create their own scores and ratings from data obtained from the CRAs as well as other sources.
Other supplied data	CRAs receive data from reputable commercial sources. This includes phone number data and politically exposed persons (PEPs) and sanctions data.	CRAs receive this data from reputable commercial sources as agreed from time to time.
Other derived data	The CRAs produce some other kinds of data themselves to manage their databases efficiently and ensure that all the relevant data about a person is on the correct credit file. **Address links**: when a CRA detects that a person seems to have moved house, it may create and store a link between the old and new address. **Aliases**: when a CRA believes that a person has changed their name, it may record the old name alongside the new one. **Financial associations and linked people**: when a CRA believes two or more people are financially linked with each other (for example, because they have a joint account), it may record that fact. **Flags and triggers**: through analysis of other data, CRAs can add indicators to credit files. These aim to summarise particular aspects of a person's financial situation. For example, a Cifas flag protects those who've been flagged as subject to fraud, and invites additional checks as a defence against further fraud risk.	The CRAs generate this data from the data sources available to them.
Data provided by the relevant people	People sometimes provide data directly to CRAs. For example, they can ask a CRA to add a supplementary statement to their credit file if they want to explain the reason for a particular entry on the file. The right to do this is explained in Section 10.	This data is provided directly by the relevant people.

5. Who do credit reference agencies share personal data with?

This section describes the types of recipient each credit reference agency can share data with. Each CRA has its own access control processes in place. For example, before it shares data with any another organisation, to check that organisation's identity and, where applicable, to confirm where it is registered with regulators.

In many cases where an organisation uses CRA services, there will be information accessible, for example, from website or at point of application or service, to explain that an organisation may check your data with a credit reference agency (for things like identity authentication and fraud checking). In some cases, some organisations have the ability to compel CRAs, by law, to disclose certain data for certain purposes.

Members of the credit reference agency data sharing arrangements

Each organisation that shares financial data with the CRAs is also entitled to receive similar kinds of financial data contributed by other organisations. These organisations are typically banks, building societies, and other lenders, as well as other credit providers like utilities companies and mobile phone networks.

Fraud Prevention Agencies

If a CRA believes that fraud has been or might be committed, it may share data with fraud prevention agencies (FPAs). These FPAs collect, maintain and share data on known and suspected fraudulent activity. Some CRAs also act as FPAs.

Resellers, distributors and agents

CRAs sometimes use other organisations to help provide their services to clients and may provide personal data to them in connection with that purpose.

Other organisations

Some data, where permitted in accordance with industry rules or where it's public information, can be shared with other organisations that have a legitimate use for it - ID verification services, for example.

Public bodies, law enforcement and regulators

The police and other law enforcement agencies, as well as public bodies like local and central authorities and the CRAs' regulators, can sometimes request the credit reference agencies to supply them with personal data. This can be for a range of purposes such as preventing or detecting crime, fraud, apprehending or prosecuting offenders, assessing or collecting tax, investigating complaints or assessing how well a particular industry sector is working.

Processors

The CRAs may use other organisations to perform tasks on their own behalf (for example, IT service providers and call centre providers).

Individuals

People are entitled to obtain copies of the personal data the CRAs hold about them. You can find out how to do this in Section 9.

6. Where is personal data stored and sent?

The three CRAs are all based in the UK, and keep their main databases there. They may also have operations elsewhere inside and outside the European Economic Area, and personal data may be accessed from those locations too. In both cases, the personal data use in those locations is protected by European data protection standards.

Sometimes the CRAs will need to send or allow access to personal data from elsewhere in the world. This might be the case, for example, when a processor or client of the CRA is based overseas or uses overseas data centres.

While countries in the European Economic Area all ensure a high standard of data protection law, some parts of the world may not provide the same level of legal protection when it comes to personal data. As a result, when a CRA does send personal data overseas it will make sure suitable safeguards are in place in accordance with European data protection requirements, to protect the data. For example, these safeguards might include:

- Sending the data to a country that's been approved by the European authorities as having a suitably high standard of data protection law. Examples include the Isle of Man, Switzerland and Canada.
- Putting in place a contract with the recipient containing terms approved by the European authorities as providing a suitable level of protection.
- Sending the data to an organisation which is a member of a scheme that's been approved by the European authorities as providing a suitable level of protection. One example is the Privacy Shield scheme agreed between the European and US authorities. Another example is Binding Corporate Rules.

If your data has been sent overseas like this, you can find out more about the safeguards used from the CRAs, whose contact details are in Section 1 above.

7. For How Long Is Personal Data Retained?

Identifiers

Identification data like names and addresses are kept while there's a continuing need to keep it. This need will be assessed on a regular basis, and data that's no longer needed for any purpose will be disposed of.

Financial accounts and repayment data

Data about live and settled accounts is kept on credit files for six years from the date they're settled or closed. If the account is recorded as defaulted, the data is kept for six years from the date of the default.

Court judgments, decrees and administration orders

Generally, court judgments and other decrees and orders are kept on credit files for six years from the date of the judgment, decree or order. But, they can be removed if the debt is repaid within one calendar month of the original date or if the judgment is set aside or recalled by the courts.

Bankruptcies, IVAs, debt relief orders and similar events

Data about bankruptcies, IVAs and other insolvency-related events and arrangements are usually kept on credit files for six years from the date they begin. This period is extended if they last longer than six years. Some data, such as a bankruptcy restrictions order, can also remain on the credit file for longer than six years.

Although the start of these events is automatically reported to the CRAs, the end (such as a discharge from bankruptcy or completion of an IVA) might not be. This is why people are advised to contact the CRAs when this happens to make sure their credit files are updated accordingly.

Search footprints

The CRAs keep search footprints for different lengths of time. Experian and Equifax keep most search footprints for one year from the date of the search, although they keep debt collection searches for up to two years. TransUnion keeps search footprints for two years from the date of the search.

Scores and ratings

CRAs may keep credit scores and credit ratings for as long as they keep a credit file about the relevant person.

Derived or created data

CRAs also create data, and links and matches between data. For example, CRAs keep address links and aliases for as long as they're considered relevant for credit referencing purposes.

Links between people are kept on credit files for as long as the CRA believes those individuals continue to be financially connected. When two people stop being financially connected, either can write to the CRA and ask for the link to be removed. The CRA will then follow a process to check the people are no longer associated with each other.

Other data

Other third party supplied data such as politically exposed persons (PEPs) and sanctions data and mortality data will be stored for a period determined by criteria such as the agreed contractual terms.

Archived data

CRAs may hold data in an archived form for longer than the periods described above, for things like research and development, analytics and analysis, (including refining lending and fraud strategies, scorecard development and other analysis such as loss forecasting), for audit purposes, and as appropriate for establishment, exercise or defence or legal claims. The criteria used to determine the storage period will include the legal limitation of liability period, agreed contractual provisions, applicable regulatory requirements and industry standards.

8. Do the credit reference agencies make decisions about me or profile me?

Lending decisions

CRAs don't tell a lender if it should offer you credit – this is for the lender to decide. Credit reference agencies provide data and analytics that help lenders make decisions about lending. The scoring tools and data CRAs provide may profile you, and are often a valuable tool in the lender's overall processes and with the criteria they use to make their decisions. A lender's own data, knowledge, processes and practices will also generally play a significant role in that lender's business decisions – and lender decisions will always remain for lenders to make.

The same analytics from a CRA may lead to different decisions from different lenders, as they can place differing importance on some factors than others. That's why you may receive a "yes" from one lender but a "no" from another.

The data CRAs provide is just one of the things that a lender might take into account when they make a lending decision. The lender might also take into account data provided by the person applying for credit, as well as any other data available to the lender from other sources. Each lender will have its own criteria for deciding whether or not to lend.

Scores and ratings

When requested, CRAs do use the data they obtain to produce credit, risk, fraud, identity, affordability, screening, collection and/or insolvency scores and credit ratings; these are explained in Section 4. CRAs don't tell a lender if it should offer you credit – this is for the lender to decide. Each credit reference agency, and each lender, will have its own criteria for how to calculate a credit score, but the following factors will usually have an effect:

- How long the person has lived at their address.
- The number and type of credit agreements and how they use those credit products.
- Whether the person has been late making payments.
- Whether the person has had any court judgments made against them.
- Whether the person has been bankrupt or had an IVA or other form of debt-related arrangement.

The CRAs may provide or make available further information on profiling where necessary from time to time.

9. What can I do if I want to see the personal data held about me? Do I have a 'portability right' in connection with my bureau data?

Data access right

You have a right to find out what personal data the credit reference agencies hold about you.

Each CRA provides more information about access rights on their websites.

TransUnion	To get online information: **https://www.transunion.co.uk/consumer-solutions/contact-us#** To make a request by post: TransUnion Information Group Limited, Consumer Services Team, PO Box 491, Leeds, LS3 1WZ
Equifax	To get online information: **https://www.equifax.co.uk** To make a request by post: Equifax Ltd, Customer Service Centre, PO Box 10036, Leicester, LE3 4FS.
Experian	To get online information: **http://www.experian.co.uk/consumer/contact-us/index.html** To make a request by post: Customer Support Centre, Experian Ltd, PO BOX 9000, Nottingham, NG80 7WF

NOTE: The information in this document will be effective from the Adopted Date set out on the first page, except for the information in this Section 9 (data portability right), and in Sections 11 and 12. These Sections provide information on new rights that will only come into effect from the 25 May 2018, which is the effective date of the General Data Protection Regulation (GDPR).

Data portability right

New data protection legislation also contains a right to data portability that may give consumers a right in some data processing contexts, to receive their personal data in a portable format when it's processed on certain grounds, such as consent. This is not a right that will apply to bureau data because this data is processed on the grounds of legitimate interests. To find out more about legitimate interests please go to Section 3.

10. What can I do if my personal data is wrong?

When the CRAs receive personal data, they perform lots of checks on it to try and detect any defects or mistakes. Ultimately, though, the credit reference agencies rely on the suppliers to provide accurate data.

If you think that any personal data a CRA holds about you is wrong or incomplete, you have the right to challenge it. It's worth knowing that the CRA won't have the right to change the data without permission from the organisation that supplied it, so the credit reference agency will need to take reasonable steps to check the data first, such as asking the organisation that supplied it to check and confirm its accuracy.

If the data does turn out to be wrong, the CRA will update its records accordingly. If the CRA still believes the data is correct after completing their checks, they'll continue to hold and keep it - although you can ask them to add a note to your file indicating that you disagree or providing an explanation of the circumstances.

If you'd like to do this, you should contact the relevant CRA using their contact details in section 1.

11. Can I object to the use of my personal data and have it deleted?

NOTE: The information in this document will be effective from the Adopted Date set out on the first page, except for the information in Sections 9, (data portability right), Section 11 and in this Section 12. These Sections provide information on new rights that will only come into effect from the 25 May 2018, which is the effective date of the General Data Protection Regulation (GDPR).

This section helps you understand how to use your data protection rights to object to your personal data being used and how to ask for it to be deleted, in connection with bureau data.

To understand these rights and how they apply to the processing of bureau data, it's important to know that the CRAs hold and process personal information in bureau data under the Legitimate Interests ground for processing (see section 4 for more information about this), and don't rely on consent for this processing.

You have the right to lodge an objection about the processing of your personal data to a CRA. If you want to do this, you should contact the relevant CRA using the contact details set out in section 1.

Whilst you have complete freedom to contact a CRA with your objection at any time, you should know that under the General Data Protection Regulation, your right to object doesn't automatically lead to a requirement for processing to stop, or for personal data to be deleted, in all cases.

Please note that, because of the importance of the credit referencing industry to the UK's financial system, and the important purposes the personal data is needed for (like supporting responsible lending, and preventing over indebtedness, fraud and money laundering) it will be very rare that the CRAs do not have compelling, overriding grounds to carry on using the personal data following an objection. In many cases, it won't be appropriate for the CRAs to restrict or to stop processing or delete bureau data, for example, where the result would be to hide a poor credit history that could enable a person or organisation to get credit they otherwise wouldn't be eligible for.

12. Can I restrict what the credit reference agencies do with my personal data?

NOTE: The information in this document will be effective from the Adopted Date set out on the first page, except for the information in Sections 9, (data portability right), Section 11 and in this Section 12. These Sections provide information on new rights that will only come into effect from the 25 May 2018, which is the effective date of the General Data Protection Regulation (GDPR).

In some circumstances, you can ask credit reference agencies to restrict how they use your personal data. Your rights are set out at Article 18 of the GDPR. You can find the contact details for each CRA in section 1.

This is not an absolute right, and your personal data may still be processed where certain grounds exist. This is:

- With your consent;
- For the establishment, exercise, or defence of legal claims;
- For the protection of the rights of another natural or legal person;
- For reasons of important public interest.

Only one of these grounds needs to be demonstrated to continue data processing.

The CRAs will consider and respond to requests they receive, including assessing the applicability of these exemptions.

Please note that given the importance of complete and accurate credit records, for purposes including for responsible lending, it will usually be appropriate to continue processing credit report data -in particular, to protect the rights of another natural or legal person, or because it's an important public interest of the union or member state.

13. Who can I complain to if I'm unhappy about the use of my personal data?

Each credit reference agency tries to ensure they deliver the best customer service levels but if you're not happy you should contact them so they can investigate your concerns.

Credit reference agency	Contact details
TransUnion Limited	**Post** TransUnion Information Group Limited, One Park Lane, Leeds, West Yorkshire LS3 1EP.
	Email consumer@transunion.co.uk
	Phone 0330 024 7574
Equifax Limited	**Post** Equifax Ltd, Customer Service Centre PO Box 10036, Leicester, LE3 4FS.
	Email complaints@equifax.com
	Phone 0333 321 4043 or 0800 014 2955
Experian Limited	**Post** Experian, PO BOX 9000, Nottingham, NG80 7WF.
	Email complaints@uk.experian.com
	Phone 0344 481 0800 or 0800 013 8888

If you're unhappy with how the CRA has investigated your complaint, you have the right to refer it to the Financial Ombudsman Service (Ombudsman) for free. The Ombudsman is an independent public body that aims to resolve disputes between consumers and businesses like CRAs. You can contact them by:

1. Phone on 0300 123 9 123 (or from outside the UK on +44 20 7964 1000)
2. Email on complaint.info@financial-ombudsman.org.uk
3. Writing to Financial Ombudsman Service, Exchange Tower London E14 9SR
4. Going to their website at www.financial-ombudsman.org.uk

You can also refer your concerns to the Information Commissioner's Office (or ICO), the body that regulates the handling of personal data in the UK. You can contact them by:

1. Phone on 0303 123 1113
2. Writing to them at Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, SK9 5AF
3. Going to their website at **www.ico.org.uk**

14. Where can I find out more?

The work credit reference agencies do is very complex, and this document is intended to provide only a concise overview of the key points. More information about each CRA and what it does with personal data is available at the following locations:

- TransUnion: **https://www.transunion.co.uk/consumer-solutions/contact-us#**
- Equifax: **https://www.equifax.co.uk/index.html**
- Experian: **https://www.experian.co.uk/**

The Information Commissioner's Office also publishes advice and information for consumers in its Credit Explained leaflet, available at https://ico.org.uk/media/forthepublic/documents/1282/credit-explained-dp-guidance.pdf.

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.

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:

	**By phone** Call us on **0800 5871 111 (or +441908 937222 if calling from abroad).** To maintain a quality service we may maintain or record phone calls for training and security purposes.
	**Using Online Banking** Log on to your Online Banking and update your details in the 'My Details & Settings' tab. Choose 'Change personal details' from the left hand menu and then click 'Change address': ■ Enter your new details (including postcode) and follow the onscreen instructions. ■ You'll need to enter a One Time Passcode (OTP) to complete this change, so make sure you have your mobile phone to hand. Please note: you must **never** share a OTP with another person, not even a cahoot employee. If the change you want to make is not covered under 'Change personal details' option , please contact us by logging on to your Online Banking and use our secure messaging service or by calling us on **0800 5871 111** (or **+441908 937222** if calling from abroad).
	**By post** Complete a 'Change of details form' from cahoot.com and return to us at the address below, along with a copy of signature bearing identification such as full UK driving license or valid EEAA passport (this includes a UK passport). **cahoot** 9 Nelson Street Bradford BD1 5XS If the change of details form does not cover the data that you want to be corrected then please call us on **0800 5871 111** (or **+441908 937222** if calling from abroad).

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.

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

	**By phone** Call us on **0800 5871 111 (or +441908 937222 if calling from abroad).** To maintain a quality service we may maintain or record phone calls for training and security purposes.
	**Using Online Banking** Log on to your Online Banking and use our secure messaging service, providing as much detail as possible about your request along with your name, address, account number, telephone number and a convenient time for us to discuss if we need to contact you.
	**By post** Write to us: cahoot 9 Nelson Street Bradford BD1 5XS

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 restrict processing you can contact us:

	**By phone** Call us on **0800 5871 111 (or +441908 937222 if calling from abroad).** To maintain a quality service we may maintain or record phone calls for training and security purposes.
	**Using Online Banking** Log on to your Online Banking and use our secure messaging service, providing as much detail as possible about your request along with your name, address, account number, telephone number and a convenient time for us to discuss if we need to contact you.
	**By post** Write to us: cahoot 9 Nelson Street Bradford BD1 5XS

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 is 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:

	**By phone** Call us on **0800 5871 111 (or +441908 937222 if calling from abroad).** To maintain a quality service we may maintain or record phone calls for training and security purposes.
	**Using Online Banking** Log on to your Online Banking and use our secure messaging service, providing as much detail as possible about your request along with your name, address, account number, telephone number and a convenient time for us to discuss if we need to contact you.
	**By post** Write to us: cahoot 9 Nelson Street Bradford BD1 5XS

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 your joint account, you'll only receive your own personal and transactional data and only if you have transactional access on the account. Other joint account customers on the same account will need to make a separate request.

To request a right to portability you can contact us:

	**By phone** Call us on **0800 5871 111 (or +441908 937222 if calling from abroad).** To maintain a quality service we may maintain or record phone calls for training and security purposes.
	**Using Online Banking** Log on to your Online Banking and use our secure messaging service, providing as much detail as possible about your request along with your name, address, account number, telephone number and a convenient time for us to discuss if we need to contact you.
	**By post** Write to us: cahoot 9 Nelson Street Bradford BD1 5XS

Changing your marketing preferences

If you'd prefer not 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 change your marketing preferences you can contact us:

	**By phone** Call us on **0800 5871 111 (or +441908 937222 if calling from abroad).** To maintain a quality service we may maintain or record phone calls for training and security purposes.
	**Using Online Banking** Log on to your Online Banking and use our secure messaging service, providing as much detail as possible about your request along with your name, address, account number, telephone number and a convenient time for us to discuss if we need to contact you.
	**By post** Write to us: cahoot 9 Nelson Street Bradford BD1 5XS

Text or email opt-out

If you receive marketing emails or SMS and don't want to in future, please use the unsubscribe link within the email and we'll 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); 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.

Please note that we don't recommend that you contact us using unsecured communication channels like normal email or social media to make requests as these are insecure.

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

Call us on **0800 587 1111 (or +441908 937222 if calling from abroad).**

To maintain a quality service we may maintain or record phone calls for training and security purposes.

Using Online Banking

Log on to your Online Banking and use our secure messaging service, providing as much detail as possible about what's gone wrong, along with your name, address, account number, telephone number and a convenient time for us to discuss your complaint.

By post

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.

Complaints
cahoot
9 nelson Street
Bradford
BD1 5XS

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 **cahoot.com**.

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.**

Alternatively, if you originally purchased your product with us online, you could submit your complaint through the European Commission's Online Dispute Resolution website. The European Commission may ultimately forward your complaint to the Financial Ombudsman Service. You can find out more information at **ec.europa.eu/odr**.

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.

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

By post

Write to us at the address below, providing:

- a daytime phone number in case we need to contact you to discuss your request;
- your sort code and account number(s); and
- detail on what information you are requesting.

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.

Subject Access Requests
cahoot
9 nelson Street
Bradford
BD1 5XS

By phone

Call us on **0800 587 1111 (or +441908 937222 if calling from abroad).**

To maintain a quality service we may maintain or record phone calls for training and security purposes.

Using Online Banking

Log on to your Online Banking and use our secure messaging service, providing as much detail as possible about what's gone wrong, along with your name, address, account number, telephone number and a convenient time for us to discuss your subject access request.

Please note that we don't recommend that you contact us using unsecured communication channels like normal email or social media to make requests as these are insecure.

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.

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 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.

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.