

PRIVACY NOTICE

Last updated April 2018

HOW WE USE YOUR PERSONAL INFORMATION

Your information will be held by Bank of Scotland plc which trades as Birmingham Midshires. BM Solutions is a brand of Birmingham Midshires. Bank of Scotland is part of the Lloyds Banking Group. This privacy notice is to let you know how companies within the Group promise to look after your personal information. This includes what you tell us about yourself, what we learn by having you as a customer, and the choices you give us about what marketing you want us to send you. This notice also tells you about your privacy rights and how the law protects you.

OUR PRIVACY PROMISE

We promise:

- To keep your data safe and private.
- Not to sell your data.
- To give you ways to manage and review your marketing choices at any time.

The privacy notice is arranged in three sections:

Personal information and the law

This section tells you who we are, what your personal information is, and how we get it. It explains how the law protects you by controlling what is allowed to happen to it.

1. Who we are	4
2. How the law protects you	4
3. Groups of Personal Information	8
4. Where we collect personal information from	10
5. How long we keep your personal information	11
6. If you choose not to give personal information	12
7. Cookies	12

The control you have

This section covers how to complain or withdraw your consent. It also tells you how you can get a copy of your personal information, or ask for it to be changed or removed.

8. How to complain	13
9. How to withdraw your consent	13
10. Letting us know if your personal information is incorrect	14
11. How to get a copy of your personal information	14
12. Your rights	15

How personal information is used

This tells you who we share personal information with. It explains what it's used for in marketing, to provide credit and to combat fraud – and how this can affect you.

13. Who we share your personal information with	16
14. How we work out what marketing you receive	18
15. How we use your information to make automated decisions	19
16. Credit Reference Agencies (CRAs)	20
17. Fraud prevention agencies	22
18. Sending data outside of the EEA	24

Personal information and the law

1. Who we are

This section gives you the legal name of the company who holds your personal information – known as the 'legal entity' – and tells you how you can get in touch with us.

Lloyds Banking Group is made up of a mix of companies, set up on different legal entities. We'll let you know which you have a relationship with, when you take out a product or service with us. You can find out more about us at www.lloydsbankinggroup.com

Contacting us about data privacy

Please use these details to contact us about any of the topics set out in this Privacy notice.

If you have any questions, or want more details about how we use your personal information, you can call us on **0345 850 5000** (+44 1422 861005 from outside the UK).

Lines are open Monday to Friday 8:00am – 6:00pm.

Calls may be monitored or recorded.

These are our main contact details. Some sections of this notice have special contact details that you can use instead.

If you are not satisfied with our response, you can contact our Group Data Protection Officer:

2. How the law protects you

This section sets out the legal reasons we rely on, for each of the ways we may use your personal information.

As well as our Privacy Promise, your privacy is protected by law. This section explains how that works.

Data Protection law says that we are allowed to use personal information only if we have a proper reason to do so. This includes sharing it outside Lloyds Banking Group. The law says we must have one or more of these reasons:

- To fulfil a contract we have with you, or
- When it is our legal duty, or
- When it is in our legitimate interest, or
- When you consent to it.

When we have a business or commercial reason of our own to use your information, this is called a 'legitimate interest'. We will tell you what that is, if we are going to rely on it as the reason for using your data. Even then, it must not unfairly go against your interests.

The law and other regulations treat some types of sensitive personal information as special. This includes information about racial or ethnic origin, sexual orientation, religious beliefs, trade union membership, health data, and criminal records. We will not collect or use these types of data without your consent unless the law allows us to do so. If we do, it will only be when it is necessary:

- For reasons of substantial public interest, or
- To establish, exercise or defend legal claims.

Here is a list of all the ways that we may use your personal information, and which of the reasons we rely on to do so. This is also where we tell you what our legitimate interests are.

What we use your personal information for:	Our reasons	Our legitimate interests
Serving you as a customer		
<ul style="list-style-type: none"> • To manage our relationship with you or your business. • To develop and carry out marketing activities. • To study how our customers use products and services from us and other organisations. • To communicate with you about our products and services. • To develop and manage our brands, products and services. 	<ul style="list-style-type: none"> • Your consent • Fulfilling contracts • Our legitimate interests • Our legal duty 	<ul style="list-style-type: none"> • Keeping our records up to date, working out which of our products and services may interest you and telling you about them. • Developing products and services, and what we charge for them. • Defining types of customers for new products or services. • Seeking your consent when we need it to contact you. • Being efficient about how we fulfil our legal and contractual duties.
Business improvement		
<ul style="list-style-type: none"> • To test new products. • To manage how we work with other companies that provide services to us and our customers. • To develop new ways to meet our customers' needs and to grow our business. 	<ul style="list-style-type: none"> • Fulfilling contracts • Our legitimate interests • Our legal duty 	<ul style="list-style-type: none"> • Developing products and services, and what we charge for them. • Defining types of customers for new products or services. • Being efficient about how we fulfil our legal and contractual duties.

What we use your personal information for:	Our reasons	Our legitimate interests
Managing our operations		
<ul style="list-style-type: none"> • To deliver our products and services. • To make and manage customer payments. • To manage fees, charges and interest due on customer accounts. • To collect and recover money that is owed to us. • To manage and provide treasury and investment products and services. 	<ul style="list-style-type: none"> • Fulfilling contracts • Our legitimate interests • Our legal duty 	<ul style="list-style-type: none"> • Being efficient about how we fulfil our legal and contractual duties. • Complying with rules and guidance from regulators.
Managing security, risk and crime prevention		
<ul style="list-style-type: none"> • To detect, investigate, report, and seek to prevent financial crime. • To manage risk for us and our customers. • To obey laws and regulations that apply to us. • To respond to complaints and seek to resolve them. 	<ul style="list-style-type: none"> • Fulfilling contracts • Our legitimate interests • Our legal duty 	<ul style="list-style-type: none"> • Developing and improving how we deal with financial crime, as well as doing our legal duties in this respect. • Complying with rules and guidance from regulators. • Being efficient about how we fulfil our legal and contractual duties.
Business management		
<ul style="list-style-type: none"> • To run our business in an efficient and proper way. This includes managing our financial position, business capability, planning, adding and testing systems and processes, managing communications, corporate governance, and audit. 	<ul style="list-style-type: none"> • Our legitimate interests • Our legal duty 	<ul style="list-style-type: none"> • Complying with rules and guidance from regulators. • Being efficient about how we fulfil our legal and contractual duties.
<ul style="list-style-type: none"> • To exercise our rights set out in agreements or contracts. 	<ul style="list-style-type: none"> • Fulfilling contracts 	

What we use your personal information for:	Our reasons	Our legitimate interests
For processing special categories of personal data		
<ul style="list-style-type: none"> • Substantial public interest 	<ul style="list-style-type: none"> • Using criminal records data to help prevent, detect, and prosecute unlawful acts and fraudulent behaviour. • Using criminal and health information as needed to provide insurance products. 	
<ul style="list-style-type: none"> • Responding to regulatory requirements 	<ul style="list-style-type: none"> • Showing whether we have assessed your situation in the right way. • Passing information to the regulator as needed to allow investigation into whether we have acted in the right way. 	
<ul style="list-style-type: none"> • Legal claims 	<ul style="list-style-type: none"> • Using any special categories of data as needed to establish, exercise or defend legal claims. 	
<ul style="list-style-type: none"> • Consent 	<ul style="list-style-type: none"> • Telling you that we need your consent to process special categories of personal data, when that is what we rely on for doing so. 	

3. Groups of personal information

This explains what all the different types of personal information mean, that are covered by data protection law.

We use many different kinds of personal information. They are grouped together like this. The groups are all listed here so that you can see what we may know about you, even if we simply get it from seeing which shops you buy things in. We don't use all this data in the same way. Some of it is useful for marketing, or for providing services to you. But some of it is private and sensitive and we treat it that way.

Type of personal information	Description
Financial	Your financial position, status and history.
Contact	Your name, where you live and how to contact you.
Socio-Demographic	This includes details about your work or profession, nationality, education and where you fit into general social or income groupings.
Transactional	Details about payments to and from your accounts with us, and insurance claims you make.
Contractual	Details about the products or services we provide to you.
Locational	Data we get about where you are. This may come from your mobile phone or the place where you connect a computer to the internet. It can also include shops where you buy something with your card.
Behavioural	Details about how you use products and services from us and other organisations.
Technical	Details on the devices and technology you use.
Communications	What we learn about you from letters and emails you write to us, and conversations between us.
Social Relationships	Your family, friends, and other relationships.
Open Data and Public Records	Details about you that are in public records such as the Electoral Register, and information about you that is openly available on the internet.
Usage Data	Other data about how you use our products and services.

Type of personal information	Description
Documentary Data	Details about you that are stored in documents in different formats, or copies of them. This could include things like your passport, driving licence, or birth certificate.
Special categories of data	<p>The law and other regulations treat some types of personal information as special. We will only collect and use these if the law allows us to do so:</p> <ul style="list-style-type: none"> • Racial or ethnic origin • Religious, political or philosophical beliefs • Trade union membership • Genetic and bio-metric data • Health data • Lifestyle information, including data related to sex life or sexual orientation • Criminal records of convictions and offences • Allegations of criminal offences. <p>You can read how we may use special types of data in the table 'How the law protects you'.</p>
Consents	Any permissions, consents, or preferences that you give us. This includes things like how you want us to contact you, whether you get paper statements, or if you prefer large-print formats.
National Identifier	A number or code given to you by a government to identify who you are, such as a National Insurance or social security number, or Tax Identification Number (TIN).

4. Where we collect personal information from

This section lists all the places where we get data that counts as part of your personal information.

We may collect personal information about you (or your business) from other Lloyds Banking Group companies and any of these sources:

Data you give to us

- When you apply for our products and services
- When you talk to us on the phone, face to face, or in branch, including recorded calls and notes we make
- When you use our websites, mobile device apps, web chat or SignVideo services
- In emails and letters
- In insurance claims or other documents
- In financial reviews and interviews
- In customer surveys
- If you take part in our competitions or promotions.

Data we collect when you use our services

This covers two things: details about how and where you access our services, and account activity that is shown on your statement.

- Payment and transaction data
This includes the amount, frequency, type, location, origin and recipients. If you borrow money, it also includes details of repayments and whether they are made on time and in full.
- Profile and usage data
This includes the security details you create and use to connect to our services. It also includes your settings and marketing choices. We also gather data from the devices you use (such as computers and mobile phones) to connect to our internet, mobile and telephone banking services. We also use cookies and other internet tracking software to collect data while you are using our websites or mobile apps. You can find out more about this in our Cookies Policy at www.bmsolutions.co.uk/cookie-policy

Data from outside organisations

- Companies that introduce you to us (such as a store or car dealership offering finance deals through us)
- Financial advisers
- Credit card providers like Visa and Mastercard
- Credit reference agencies such as Callcredit, Equifax and Experian
- Insurers
- Retailers
- Comparison websites

- Social networks (for instance, when you click on one of our Facebook or Google ads)
- Fraud prevention agencies
- Other financial services companies (to help prevent, detect and prosecute unlawful acts and fraudulent behaviour)
- Employers (for instance, to get a reference if you apply for a mortgage)
- Payroll service providers
- Land agents (such as firms who do property valuations for mortgages)
- Public information sources such as the Electoral Register or Companies House
- Loyalty schemes like Avios or Everyday Offers
- Agents, suppliers, sub-contractors and advisers
These can be types of firm we use to help us run accounts and services. They can also be specialist companies who advise us on ways to develop and improve our business.
- Market researchers (who combine data from many sources to produce market trend reports and advice.)
- Medical professionals*
- Government and law enforcement agencies.

* For some insurance products, we may ask your GP or other medical practitioner to send us a report. We will only do this if we get your consent first.

5. How long we keep your personal information

This section explains how long we may keep your information for and why.

We will keep your personal information for as long as you are a customer of Lloyds Banking Group.

We may keep your data for up to 10 years after you stop being a customer. The reasons we may do this are:

- To respond to a question or complaint, or to show whether we gave you fair treatment.
- To study customer data as part of our own internal research.
- To obey rules that apply to us about keeping records.

We may also keep your data for longer than 10 years if we cannot delete it for legal, regulatory or technical reasons. As an example, we have to hold pension transfer information indefinitely; and in cases of subsidence* we will keep insurance claims data for up to 15 years after you stop being a customer.

We will only use your personal information for those purposes and will make sure that your privacy is protected.

* Subsidence is when a building becomes unsafe or damaged by ground sinking around it.

6. If you choose not to give personal information

You can choose not to give us personal information. In this section we explain the effects this may have.

We may need to collect personal information by law, or to enter into or fulfil a contract we have with you.

If you choose not to give us this personal information, it may delay or prevent us from fulfilling our contract with you, or doing what we must do by law. It may also mean that we cannot run your accounts or policies. It could mean that we cancel a product or service you have with us.

We sometimes ask for information that is useful, but not required by law or a contract. We will make this clear when we ask for it. You do not have to give us these extra details and it won't affect the products or services you have with us.

7. Cookies

This section contains a link to our Cookies Policy.

Cookies are small computer files that get sent down to your PC, tablet or mobile phone by websites when you visit them. They stay on your device and get sent back to the website they came from, when you go there again. Cookies store information about your visits to that website, such as your choices and other details. Some of this data does not contain personal details about you or your business, but it is still protected by this Privacy notice.

To find out more about how we use cookies, please see our Cookies Policy at www.bmsolutions.co.uk/cookie-policy

The control you have

8. How to complain

This section gives details of how to contact us to make a complaint about data privacy. It also shows you where you can get in touch with the government regulator.

Please let us know if you are unhappy with how we have used your personal information. You can call us on **0345 300 2627**.

Lines are open 8:00am to 6:00pm Monday to Friday.

Calls may be monitored or recorded.

Or you can write to us at:

Birmingham Midshires
Pendeford Business Park
Wobaston Road
Wolverhampton
WV9 5HA

You also have the right to complain to the regulator, and to lodge an appeal if you are not happy with the outcome of a complaint.

In the UK this is the Information Commissioner's Office. Find out on their website www.ico.org.uk/concerns how to report a concern or call **0303 123 1113**.

In Jersey, please contact the Office of the Information Commissioner at www.oicjersey.org/online-enquiry/#/complain/form or call **01534 716 530**

In Guernsey, please contact the Office of the Data Protection Commissioner at www.dataci.gg/online-enquiry/#/complain/form or call **01481 742 074**

In Isle of Man, please contact the Information Commissioner at www.inforights.im/contact-us or call **01624 693 260**

9. How to withdraw your consent

This section explains what to do if you no longer want us to hold or use your personal information.

You can withdraw your consent at any time. If you want to do so, please call us on **0345 850 5000 (+44 1422 861005** from outside the UK).

Lines are open Monday to Friday 8:00am – 6:00pm.

Calls may be monitored or recorded.

This will only affect the way we use information when our reason for doing so is that we have your consent. See the section 'Your Rights' about more generally restricting use of your information.

If you withdraw your consent, we may not be able to provide certain products or services to you. If this is so, we will tell you.

10. Letting us know if your personal information is incorrect

Here you can find out how to contact us if you think the information we hold for you is wrong, incomplete or out of date.

You have the right to question any information we have about you that you think is incorrect. We'll take reasonable steps to check this for you and correct it.

If you want to do this, please call us on **0345 850 5000 (+44 1422 861005)** from outside the UK).

Lines are open Monday to Friday 8:00am – 6:00pm.

Calls may be monitored or recorded.

11. How to get a copy of your personal information

This section tells you where to write to us to get a copy of your personal information, and how to ask for a digital file you can use yourself or share easily with others.

You can get a copy of all the personal information we hold about you by writing to us at this address:

HBOS DSAR
Charlton Place, (C43)
Charlton Road
Andover
Hants
SP10 1RE

When you want to share your data with outside companies

You also have the right to get certain personal information from us as a digital file, so you can keep and use it yourself, and give it to other organisations if you choose to. If you wish, we will provide it to you in an electronic format that can be easily re-used, or you can ask us to pass it on to other organisations for you.

If you want to do this, please call us on **0345 850 5000 (+44 1422 861005)** from outside the UK).

Lines are open Monday to Friday 8:00am – 6:00pm.

Calls may be monitored or recorded.

12. Your rights

What if you want us to stop using your personal information? This section explains about your right to object and other data privacy rights you have – as well as how to contact us about them.

You can object to us keeping or using your personal information. This is known as the 'right to object'.

You can also ask us to delete, remove, or stop using your personal information if there is no need for us to keep it. This is known as the 'right to erasure' or the 'right to be forgotten'.

There may be legal or other official reasons why we need to keep or use your data. But please tell us if you think that we should not be using it.

We may sometimes be able to restrict the use of your data. This means that it can only be used for certain things, such as legal claims or to exercise legal rights.

You can ask us to restrict the use of your personal information if:

- It is not accurate
- It has been used unlawfully but you don't want us to delete it
- It is not relevant any more, but you want us to keep it for use in legal claims
- You have already asked us to stop using your data but you are waiting for us to tell you if we are allowed to keep on using it.

If we do restrict your information in this way, we will not use or share it in other ways while it is restricted.

If you want to object to how we use your data, or ask us to delete it or restrict how we use it or, please call us on **0345 850 5000 (+44 1422 861005** from outside the UK).

Lines are open Monday to Friday 8:00am – 6:00pm.

Calls may be monitored or recorded.

How personal information is used

13. Who we share your personal information with

We may share your personal information with outside organisations such as credit card providers, insurers or tax authorities. This is so that we can provide you with products and services, run our business, and obey rules that apply to us. Here we list all the types of organisation that we may share your personal information with.

Lloyds Banking Group

We may share your personal information with other companies in Lloyds Banking Group.

Authorities

This means official bodies that include:

- Central and local government
- HM Revenue & Customs, regulators and other tax authorities
- UK Financial Services Compensation Scheme and other deposit guarantee schemes
- Law enforcement and fraud prevention agencies.

Banking and financial services

Outside companies we work with to provide services to you and to run our business.

- Agents, suppliers, sub-contractors and advisers
These are types of firm that we use to help us run accounts, policies and services.
- Agents who help us to collect what is owed to us
- Credit reference agencies (such as Callcredit, Equifax and Experian)
- Someone linked with you or your business's product or service.
This could mean a joint account holder, trustee, or fellow company director.
- Other financial services companies (to help prevent, detect and prosecute unlawful acts and fraudulent behaviour)
- Independent Financial Advisors.
This could be someone who advises you on things like pensions or life assurance. We won't share any personal information unless they have your consent to ask us for it.
- Price comparison websites and similar companies.
- Employers (for instance, to confirm your identity if we ask for a mortgage reference)
- Companies you ask us to share your data with
This is to do with something called Open Banking, which gives you more freedom and control to use your own banking data. It can make it easier for you or your business to shop around for products like credit cards, savings and current accounts. You can find out more at www.openbanking.org.uk

Insurers

We share personal information with insurance industry companies to process claims and help reduce fraud. We do that in these ways:

- If you apply for insurance through us, we may pass your personal or business details to the insurer.
- If you apply for insurance with us as the insurer, we may share your personal or business details with reinsurers.
- If you make an insurance claim, information you give to us or the insurer may be put on a register of claims. This will be shared with other insurers, our agents, suppliers and sub-contractors. In some cases we may also share it with our business partners, if you also have a relationship with them.

Other services and schemes

These are organisations that we may need to share your personal information with, because of what you can do with the product or service you have with us.

- If you have a debit, credit or charge card with us, we will share transaction details with companies which help us to provide this service (such as Visa and Mastercard).
This is needed to keep your account balance and statements up to date, for example.
- If you use direct debits, we will share your data with the Direct Debit scheme.
- If you have a product which has a loyalty scheme like Avios or Everyday Offers, we will share your data with that scheme.
- If you have a product with benefits such as travel insurance or discount offers, we will share your data with the benefit providers. We may also share it with other companies involved in how you use the service (such as a private car park operator).
- If you have a secured loan or mortgage with us, we may share information with other lenders who also hold a charge on the property (For example, the other party in a shared ownership scheme)

General business

Outside companies we use to help grow and improve our business.

- Companies we have a joint venture or agreement to co-operate with (such as a store or car dealership offering finance deals through us)
- Organisations that introduce you to us
This might be a store or car dealership that offers finance deals through us, or a price comparison website.
- Market researchers
We send data which these firms combine with data from other sources to produce market trend reports and advice.
- Advisers who help us to come up with new ways of doing business.
This might be a legal firm, IT supplier or consultancy.

Company mergers and takeovers

We may also share your personal information if the make-up of Lloyds Banking Group changes in the future:

- We may choose to sell, transfer, or merge parts of our business, or our assets. Or we may try to bring other businesses into Lloyds Banking Group.
This is sometimes called Mergers & Acquisitions or 'company takeovers'.
- During any such process, we may share your data with other parties involved. We'll only do this if they agree to keep your data safe and private.
- If the change to our Group happens, then other parties may use your data in the same way as set out in this notice.

14. How we work out what marketing you receive

We use marketing to let you know about products, services and offers that you may want from us. This section tells you how we decide what marketing to show or send you. It also explains how we work out what you may be interested in.

We may use your personal information to make decisions about what products, services and offers we think you may be interested in. This is what we mean when we talk about 'marketing'.

We can only use your personal information to send you marketing messages if we have either your consent or a 'legitimate interest'. That is when we have a business or commercial reason to use your information. It must not conflict unfairly with your own interests.

The personal information we have for you is made up of what you tell us, and data we collect when you use our services, or from outside organisations we work with. We study this to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you.

This is called profiling for marketing purposes. You can contact us at any time and ask us to stop using your personal information this way.

If you allow it, we may show or send you marketing material online (on our own and other websites including social media), in our app, or by email, mobile phone or post.

What you get will depend on marketing choices that you set. You can change these at any time and tell us to stop sending you marketing.

You can also tell us not to collect data while you are using our websites or mobile apps. If you do, you will still see some marketing but it will not be tailored to you.

See our Cookies Policy at www.bmsolutions.co.uk/cookie-policy for details about how we use this data to improve our websites and mobile apps.

Whatever you choose, you'll still receive statements and other important information such as changes to your existing products and services.

We do not sell the information we have about you to outside organisations.

We may ask you to confirm or update your choices, if you take out any new products or services with us in future. We will also ask you to do this if there are changes in the law, regulation, or the structure of our business.

If you change your mind you can contact us to update your choices at any time.

15. How we use your information to make automated decisions

Here we tell you how we use automated systems to make decisions about you and your money. We also explain the rights you have to challenge decisions made this way.

We sometimes use systems to make automated decisions about you or your business. This helps us to make sure our decisions are quick, fair, efficient and correct, based on what we know. Automated decisions can affect the products, services or features we may offer you now or in the future, or the price that we charge you for them. They are based on personal information that we have or that we are allowed to collect from others.

Here are the types of automated decision we make:

Pricing

We may decide what to charge for some products and services based on what we know. For instance, if you use our online mortgage calculator, it will use the personal financial details you put in to estimate the kind of mortgage we may offer you. If you apply for insurance, we will compare what you tell us with other records to work out how likely you are to make a claim. This will help us decide whether to offer you the product and what price to charge you.

Tailoring products, services, offers and marketing

We may place you in groups with similar customers. These are called customer segments. We use these to study and learn about our customers' needs, and to make decisions based on what we learn. This helps us to design products, services and offers for different customer segments, and to manage our relationships with them. It also helps us tailor the marketing that individuals receive or are shown on our own and other websites and mobile apps, including social media.

Detecting fraud

We use your personal information to help decide if your personal or business accounts may be being used for fraud or money-laundering. We may detect that an account is being used in ways that fraudsters work. Or we may notice that an account is being used in a way that is unusual for you or your business. If we think there is a risk of fraud, we may stop activity on the accounts or refuse access to them.

Opening accounts

When you open an account with us, we check that the product or service is relevant for you, based on what we know. We also check that you or your business meet the conditions needed to open the account. This may include checking age, residency, nationality or financial position.

Approving credit

We use a system to decide whether to lend money to you or your business, when you apply for credit such as a loan or credit card. This is called credit scoring. It uses past data to assess how you're likely to act while paying back any money you borrow. This includes data about similar accounts you may have had before.

Credit scoring uses data from three sources:

- Your application form
- Credit reference agencies
- Data we may already hold.

It gives an overall assessment based on this. Banks and other lenders use this to help us make responsible lending decisions that are fair and informed.

Credit scoring methods are tested regularly to make sure they are fair and unbiased.

Your rights

As a person you have rights over automated decisions.

- You can ask that we do not make our decision based on the automated score alone.
- You can object to an automated decision, and ask that a person reviews it.

If you want to know more about these rights, please contact us.

16. Credit Reference Agencies (CRAs)

This section explains how we work with outside companies to decide whether to lend you money through products like credit cards or loans. It explains what we do and why we do it.

We carry out credit and identity checks when you apply for a product or services for you or your business. We may use Credit Reference Agencies to help us with this.

If you use our services, from time to time we may also search information that the CRAs have, to help us manage those accounts.

We will share your personal information with CRAs and they will give us information about you. The data we exchange can include:

- Name, address and date of birth
- Credit application
- Details of any shared credit
- Financial situation and history
- Fraud prevention information
- Public information, from sources such as the Electoral Register and Companies House.

We'll use this data to:

- Assess whether you or your business is able to afford to make repayments
- Make sure what you've told us is true and correct
- Help detect and prevent financial crime
- Manage your accounts with us
- Trace and recover debts
- Tell you about relevant offers.

We will go on sharing your personal information with CRAs for as long as you are a customer. This will also include details of funds going into the account, and the account balance. If you borrow, it will also include details of your repayments and whether you repay in full and on time. We will also tell the CRAs when you settle your accounts with us. The CRAs may give this information to other organisations that want to check your credit status.

When we ask CRAs about you or your business, they will note it on your credit file. This is called a credit search. Other lenders may see this and we may see credit searches from other lenders.

If you apply for a product with someone else, we will link your records with theirs. We will do the same if you tell us you have a spouse, partner or civil partner – or that you are in business with other partners or directors.

You should tell them about this before you apply for a product or service. It is important that they know your records will be linked together, and that credit searches may be made on them.

CRAs will also link your records together. These links will stay on your files unless one of you asks the CRAs to break the link. You will normally need to give proof that you no longer have a financial link with each other.

You can find out more about the CRAs on their websites, in the Credit Reference Agency Information Notice. This includes details about:

- Who they are
- Their role as fraud prevention agencies
- The data they hold and how they use it
- How they share personal information
- How long they can keep data
- Your data protection rights.

Here are contact details for each of the three main Credit Reference Agencies:

Callcredit: www.callcredit.co.uk/crain or call **0330 024 7574**

Equifax: www.equifax.co.uk/crain or call **0333 321 4043** or **0800 014 2955**

Experian: www.experian.co.uk/crain or call **0344 481 0800** or **0800 013 8888**

17. Fraud prevention agencies

This section deals with information we share outside our group to help fight financial crime. This includes crimes such as fraud, money-laundering and terrorist financing.

We may need to confirm your identity before we provide products or services to you or your business. This may include carrying out fraud checks at the point of sale.

Once you have become a customer of ours, we will share your personal information as needed to help combat fraud and other financial crime. The organisations we share data with are:

- Registered Fraud Prevention Agencies (FPAs)
- Other agencies and bodies acting for the same purpose
- Industry databases used for this purpose
- Insurers

Throughout our relationship with you, we and these organisations exchange data between us to help prevent, deter, detect and investigate fraud and money-laundering.

None of us can use your personal information unless we have a proper reason to do so. It must be needed either for us to obey the law, or for a 'legitimate interest'.

When we have a business or commercial reason of our own to use your information, this is called a 'legitimate interest'. We will tell you what that is, if we are going to rely on it as the reason for using your data. Even then, it must not unfairly go against your interests.

We will use the information to:

- Confirm identities
- Help prevent fraud and / or money-laundering
- Fulfil any contracts you or your business has with us.

We or an FPA may allow law enforcement agencies to access your personal information. This is to support their duty to prevent, detect, investigate and prosecute crime.

These other organisations can keep personal information for different lengths of time, up to six years.

The information we use

These are some of the kinds of personal information that we use:

- Name
- Date of birth
- Residential address
- History of where you have lived
- Contact details, such as email addresses and phone numbers
- Financial data
- Whether you have been a victim of fraud
- Data about insurance claims you have made
- Data relating to your or your businesses products or services
- Employment details
- Vehicle details
- Data that identifies computers or other devices you use to connect to the internet. This includes your Internet Protocol (IP) address.

Automated decisions for fraud prevention

The information we have for you or your business is made up of what you tell us, and data we collect when you use our services, or from third parties we work with.

We and other organisations acting to prevent fraud may process your personal information in systems that look for fraud by studying patterns in the data. We may find that an account or policy is being used in ways that fraudsters work. Or we may notice that an account is being used in a way that is unusual for you or your business. Either of these could indicate a risk that fraud or money-laundering may be carried out against a customer, the bank or the insurer.

How this can affect you

If we or an FPA decide there is a risk of fraud, we may stop activity on the accounts or block access to them. FPAs and cross-industry organisations may also keep a record of the risk that you or your business may pose.

This may result in other organisations refusing to provide you with products or services, or to employ you.

Data transfers out of the EEA

FPAs and other organisations we share data with for these purposes may send personal information to countries outside the European Economic Area ('EEA'). When they do, there will be a contract in place to make sure the recipient protects the data to the same standard as the EEA. This may include following international frameworks for making data sharing secure.

18. Sending data outside the EEA

This section tells you about the safeguards that keep your personal information safe and private, if it is sent outside the EEA.

We will only send your data outside of the European Economic Area ('EEA') to:

- Follow your instructions
- Comply with a legal duty
- Work with our suppliers who help us to run your accounts and services.

If we do transfer your personal information outside the EEA to our suppliers, we will make sure that it is protected to the same extent as in the EEA. We'll use one of these safeguards:

- Transfer it to a non-EEA country with privacy laws that give the same protection as the EEA. Learn more on the European Commission Justice website http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
- Put in place a contract with the recipient that means they must protect it to the same standards as the EEA. Read more about this here on the European Commission Justice website http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
- Transfer it to organisations that are part of Privacy Shield. This is a framework that sets privacy standards for data sent between the US and EU countries. It makes sure those standards are similar to what is used within the EEA. You can find out more about data protection on the European Commission Justice website http://ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm

Birmingham Midshires is a division of Bank of Scotland plc. Registered in Scotland No. SC327000.

Registered Office: The Mound, Edinburgh EH1 1YZ. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Financial Services Register number 169628.

Telephone calls may be monitored or recorded.



56425 (05/18)

BMSOLUTIONS
FROM BIRMINGHAM MIDSHIRES