Privacy Policy

Britain's exit from the European Union (Brexit) notice

Please note that as of 31 December 2020, the European General Data Protection Regulation (GDPR) no longer directly applies in the UK. However, the UK has passed its own version into law, known as the UK GDPR (United Kingdom General Data Protection Regulation). All references to GDPR in this Policy are to the UK GDPR. The UK GDPR has equivalent legal provisions to the GDPR and your rights, and the UK Data Protection Act 2018 and other applicable legislation provide supplementary protections. Unless otherwise specified, the details within this policy will not be impacted by this change. The UK Government are seeking adequacy decisions from the European Commission and if this is so we will revisit this policy as appropriate.

Personal data may be transferred to recipients located in countries outside the UK. In particular, your personal data will be stored locally but may also be stored and backed up on servers located outside of the UK. We may also share your personal data with our trusted service providers and partners, some of which may be located outside the UK.

In accordance with applicable data protection law, we ensure that whenever we transfer your personal data outside of the UK it is protected. This is achieved by ensuring that either:

- the country outside of the UK to which your personal data is transferred has been deemed to provide an adequate level of protection for personal data by the Secretary of State; or
- the recipients of your personal data in the relevant country outside of the UK enter into standard contractual clauses which have been approved by the Secretary of State or offer other appropriate safeguards.

If you would like further information on the specific mechanism used by us when transferring your personal data outside of the UK, you can contact us using the details set out at the end of this Privacy Policy.

1. About us

We are Aldermore Bank Plc ("Aldermore"), our Company Registration number is 947662 and our Registered Office address is Apex Plaza, Forbury Road, Reading, RG1 1AX.

This PRIVACY POLICY explains how and why Aldermore use your personal data. In this Policy, when we talk about personal data, we mean any information that relates to an identifiable natural person – in this case, you. When we use terms such as "we", "us" and "our" in this Policy, we mean Aldermore.

This Policy applies to personal data processed by or collected on behalf of Aldermore. We may collect information from you when you visit our website, apply for a service, contact us by telephone or email or receive a communication from us relating to your service.

You should read this policy so you know what personal data we collect about you, what we do with it and how you can exercise your rights in connection with it. You should also read any other privacy notices that we give you, that might apply to our use of your personal data in specific circumstances from time to time.

Aldermore is a "Data Controller". This is a legal term which means that we make decisions about how and why we use your personal data. As the "Data Controller", we are responsible for making sure that your personal data is used in accordance with applicable data protection laws. As Data Controller, we are required by law to give you the information in this Policy.

However, on occasions there may be other Data Controllers involved in processing your data as further explained in this Policy, or as you may be advised at the time your information is to be processed.

At the foot of this Policy we have included links to external websites providing further information to help you. We have also included details of contact points, including those for our Data Protection Officer, which you can use if you wish to ask us for further information or to exercise your rights.

You will see at the end of this Policy that we mention the privacy notices of Fraud Prevention Agencies and Credit Reference Agencies. We do need to share these with you. Please read them carefully and contact those organisations if you have questions (their details are in their notices).

We reserve the right to change the policy at any time, so please check back regularly to keep informed of updates to this Policy.

2. Have you been introduced to us by a Broker or other Intermediary?

Our products and services are available through our regional offices and on our website as well as through professional and financial advisors and anyone else who acts as a person sitting in between you and us in relation to what we do for you. We work with brokers and intermediaries (including Packagers) for our lending and investment products and services. In this Policy we will call these persons "brokers and other intermediaries".

When a broker or other intermediary processes your personal data on our behalf, this privacy policy will apply, and you should contact our Data Protection Officer to exercise your rights under data protection laws.

When a broker or other intermediary processes your personal data as a Data Controller in its own right, its own privacy policy will apply, and you should ask them for a copy if you do not have one by the time you are introduced to us.

3. What Personal Data do we collect from you?

This will depend on the products and services you apply for and (if your application is successful) obtain from us. Generally speaking, the personal data we process about you falls into three main categories:

Who you are

- where you live and how to contact you (Tax Residency status is collected for Savings and Residential Mortgage products)
- your name
- your date of birth and/or age (so that we can, for example, make sure that you are eligible to apply for the product and it is suitable for you)
- your address and correspondence address (where different from address) and address history
- 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, if this is necessary for us to comply with our legal and regulatory requirements
- your marital status, family, lifestyle or social circumstances if relevant to the application (for example, the number of dependents you have or if you are a widow or widower)
- what we learn about you from letters, emails and conversations between us
- details on the devices and technology you use
- usage data about how you use our products and services
- personal data which we obtain from Fraud Prevention Agencies (see the section on 'Fraud Prevention Agencies' below)
- some special categories of personal data such as information about your health
- contact details such as phone and email addresses
- device identifiers including IP address
- vehicle details

Your employment status and sources of income

- whether you are employed, retired or receive benefits
- your financial position, status and history
- your salary and other sources of income
- any savings

Your financial commitments

- existing borrowings and loans
- details about payments to and from your accounts with us
- household expenditure
- personal data about your credit history which we will obtain from Credit Reference Agencies (CRAs) including data which originates from Royal Mail (UK postal addresses), local authorities (electoral roll), the insolvency service, Companies House, other lenders and providers of credit who supply data to the CRAs, court judgments, decrees and administration orders made publicly available through public registers (see information on CRAs below)

4. Joint Applicants, Guarantors and Powers of Attorney

A shortened version of this Policy is included in all paper-based, online and telephone application, proposal, and claim forms. The short version references this long version and encourages readers to review the full policy. It is important that anyone providing personal information understands how it will be used.

If you make a joint application with your spouse, partner or family member, we will also collect the personal data mentioned above about that person. You must show our privacy policy to any other applicants and ensure they confirm they know you will share their personal data with us for the purposes described in it.

If you apply for a mortgage with a guarantor, for example, that person will see a shortened version of our privacy policy when they submits their own personal data to us because they must sign the application form or provide their details in the online application.

If there is somebody who has power of attorney over your affairs, that person will see a shortened version of our privacy policy when we make contact with them directly.

5. Beneficial Owners

If you make an application for your business, we will also collect the personal data mentioned above about all individuals who you have a financial link with, for example other directors or officers of your company, who you must include on the application form.

You must show this Policy to any other applicants (including all beneficial owners and directors) and ensure they know you will share their personal data with us for the purposes described in it.

In order to assess your company's suitability for the product, we need to verify that:

- all applicants are included
- the identity for all applicants is verified
- all applicants are UK taxpayers (Applies to savings products and residential mortgages. For residential mortgages you need to have paid UK tax within the last 3 years)

To do this, we use an external agency to check all directors are included and gather publicly held data to run authentication and world checks. If the data we gather is insufficient to allow us to run these checks, we will request them directly from you.

6. Witnesses

Some of our products and services including mortgages and business finance, require witness signatures (to comply with execution formalities as a matter of law) and include the name and address of individuals who have acted as a witness for you. These details are kept on the application forms and stored with your account documents in line with our retention procedures.

As these details are not added to our operational systems, they will not be accessible, should the witness exercise their right of access (see the right to request access in the 'your rights' section of this Policy).

7. What is the source of your personal data?

Directly from you:

We will generally collect your personal data from you directly, including: Information entered into our website **www.aldermore.co.uk** ("our site") when you register to use our site or subscribe to our newsletters.

- Information we have gathered from you when we have asked you to respond to face-to-face contact, telephone calls, , video conferences, emails, letters and other correspondence you have with us
- Material you post on our social media pages
- Details of transactions you carry out through our site
- Information we have gathered from asking you to respond to surveys, although you do not have to complete them
- If you take part in our competitions or promotions

Data from third parties we work with:

- Companies that introduce you to us
- Brokers
- Credit Reference Agencies (CRAs, see below)
- Retailers
- Comparison websites
- Social networks
- Fraud Prevention Agencies (FPAs)
- Land agents
- Public information sources such as Companies House
- Agents working on our behalf
- Market researchers
- Government and law enforcement agencies

Data we collect when you use our services:

- Payment and transaction data
- We will also collect information derived from cookies, which will include your Internet Protocol (IP) address unless you have set your browser not to accept cookies
- We may collect information about your computer, including where available your IP address, operating system and browser type, for system administration and to report aggregated information to our advertisers. This is statistical data about our users' browsing actions and patterns and does not identify you as an individual
- By using our websites or applications you agree that cookies may be forwarded from the relevant website or application to your computer or device
- The cookie will enable us to know that you have visited the website or application before and will identify you. We may also use the cookie to prevent fraud
- For more information refer to our Cookie policy

From Credit Reference Agencies (CRAs):

In addition, we will obtain your personal data from Credit Reference Agencies (CRAs) which we use to verify your identity and creditworthiness (see the section below titled "Sharing Information with Credit Reference Agencies"), Fraud Prevention Agencies, your employer, landlord, other lenders, His Majesty's Revenue and Customs (HMRC), Department for Work and Pensions (DWP), publicly available directories and information (e.g. telephone directory, social media, internet, news articles).

Some of the personal data obtained from Credit Reference Agencies will have originated from publicly accessible sources. Credit Reference Agencies draw on court decisions, bankruptcy registers and the electoral register/roll. We explain more about this below.

8. What we do with your data

We collect and process your data for several purposes, and for each purpose Aldermore must explain to you what legal grounds justify our processing of your personal data. Here are the legal grounds that are relevant to us:

Processing necessary to perform our contract with you for your product or service or for taking steps prior to entering into it during the application stage:

- Administering and managing your account and associated services, updating your records, tracing your whereabouts to contact you about your account and doing this for the recovery of debt;
- Sharing your personal data with certain third-party service suppliers such as payment service providers;
- All stages and activities relevant to managing your account including enquiry, application, administration and management of accounts, illustrations, requests for transfers of equity, setting up/changing/ removing guarantors;
- To manage how we work with other companies that provide services to us and our customers
- To manage fees, charges and interest due on customer accounts
- To exercise our rights set out in agreements and contracts
- When we do, what we will call throughout this policy "profiling and other automated decision making"; by "automated decision making" we mean making decisions about you, such as;
  - your suitability for a product,
  - using a computer based and
  - automated system without a person being involved in making that decision (at least first time around)
- By "profiling" we mean doing some automated processing of your personal data to evaluate
  - personal aspects about you, such as;
  - analysing or predicting your economic situation,
  - health,
  - personal preferences,
  - interests,
  - reliability,
  - behaviour,
  - location or
  - movements.
- For more information, see the sections: "Automated Processing and Automated Decision Making" and "Profiling" below
- Preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us.

Processing necessary to comply with our legal obligations:

- To carry out identity checks, anti-money laundering checks and checks with Fraud Prevention Agencies pre-application, at the application stage and periodically after that (up to annually). Where you have been introduced to us by a broker or other intermediary, they may do these searches on our behalf
- For compliance with laws that apply to us
- For establishment, defence and enforcement of our legal rights or those of any other member of Aldermore

- For activities relating to the prevention, detection and investigation of crime
- To carry out monitoring and to keep records (see below)
- To deal with requests from you to exercise your rights under data protection laws
- To process information about a crime or offence and proceedings related to that (in practice this will be relevant if we know or suspect fraud)

When we share your personal data with these other people or organisations:

- Your guarantor (if you have one)
- Joint account holders, trustees and beneficiaries, and the person with power of attorney over your affairs
- Beneficial owners, if you are applying for a product through your company
- Other payment services providers such as when you ask us to share information about your account with them
- Other account holders or individuals when we have to provide your information to them because some money paid to you by them should not be in your account
- Fraud Prevention Agencies
- Law enforcement agencies and governmental and regulatory bodies such as HMRC, the Financial Conduct Authority, the Prudential Regulation Authority, the Ombudsman, the Information Commissioner's Office and under the Financial Services Compensation Scheme (depending on the circumstances of the sharing) and
- Courts and to other organisations where that is necessary for the administration of justice, to protect vital interests and to protect the security or integrity of our business operations

Where we consider that, on balance, it is appropriate for us to do so, processing necessary for the following legitimate interests which apply to us and in some cases other organisations (who we list below) are:

- Administering and managing your account and services relating to that, updating your records, tracing your whereabouts to contact you about your account, and doing this for recovering debt
- To test the performance of our products, services and internal processes
- To adhere to guidance and best practice under the regimes of governmental and regulatory bodies such as HMRC, the Financial Conduct Authority, the Prudential Regulation Authority, the Ombudsman, the Information Commissioner's Office and under the Financial Services Compensation Scheme
- For management and audit of our business operations including accounting
- To carry out searches at Credit Reference Agencies pre-application, at the application stage, and periodically after that (up to annually). Where you have been introduced to us by a broker or other intermediary, they may do these searches on our behalf
- To carry out monitoring and to keep records (see below)
- To administer our good governance requirements and those of other members of our Group
- For market research and analysis and developing statistics
- For some of our profiling and other automated decision making, in particular where this does not have a legal effect or otherwise significantly affect you
- We process your personal data on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us.

When we share your personal data with these other people or organisations;

- Your guarantor (if you have one)
- Joint account holders, trustees and beneficiaries and any person with power of attorney over your affairs (in each case only if relevant to you)
- Beneficial owners
- Members of our Group
- Other payment services providers such as when you ask us to share information about your account with them
- Other account holders or individuals when we have to provide your information to them because some money paid to you by them should not be in your account
- The broker or other intermediary who introduced you to us
- Our legal and other professional advisers, auditors and actuaries
- Financial institutions and trade associations
- Governmental and regulatory bodies such as HMRC, the Financial Conduct Authority, the Prudential Regulation Authority, the Ombudsman, the Information Commissioner's Office and under the Financial Services Compensation Scheme
- Tax authorities who are overseas for instance if you are subject to tax in another jurisdiction, we may share your personal data directly with relevant tax authorities overseas (instead of via HMRC)
- Other organisations and businesses who provide services to us such as debt recovery agencies, back up and server hosting providers, IT software and maintenance providers, document storage providers and suppliers of other back office functions
- Buyers and their professional representatives as part of any restructuring or sale of our business or assets
- Credit Reference Agencies (see below where we explain more) and
- Market research organisations who help us to develop and improve our products and services.

Processing with your consent

We may also from time to time ask you for your consent for other purposes, which we will explain to you at the time. For example, when you request that we share your personal data with someone else and consent to that.

For some of our processing of special categories of personal data such as about your health (and it will be explained to you when we ask for that explicit consent what purposes, sharing and use it is for).

Processing for a substantial public interest under laws that apply to us where this helps us to meet our broader social obligations such as:

- Processing of your special categories of personal data such as about your health or if you are a vulnerable customer
- Processing that we need to do to fulfil our legal obligations and regulatory requirements

When we share your personal data with other people and organisations such as members of our Group if they need to know that you are a vulnerable customer and your relatives, social services, your carer or the person who has power of attorney over your affairs.

Use of Artificial Intelligence at Aldermore

From time to time we may choose to use Artificial Intelligence (AI), to support good customer outcomes and the effective delivery of services. We do not rely solely on AI for any significant decisions related to your application or in life account reviews without appropriate and effective human intervention (for example we currently use AI to assist in directing email queries to appropriate teams, timing of outbound communication and to support the improvement of internal processes).

Some of our suppliers may use AI for the services they provide to us. Where we use suppliers to support delivery of products and services to you, these will be engaged following appropriate due diligence, risk assessment and based on contractual safeguards.

9. How and when you can withdraw your consent

Much of what we do with your personal data is not based on your consent and is instead based on other legal grounds. For processing that is based on your consent, you have the right to revoke that consent for future processing at any time. You can do this by contacting us using the contact details at the end of this document. The consequence might be that we cannot send you some marketing communications or that we cannot consider special categories of personal data such as about your health or if you are a vulnerable customer (but these outcomes will be relevant only in cases where we rely on your explicit consent for this).

We will tell the broker or other intermediary who introduced you to us that you have withdrawn your consent only if it is our data processor (this means an organisation that is processing personal data on our behalf) or if we are required to do when you exercise certain rights under data protection laws. If they are acting as a Data Controller in their own right, you should make sure to contact them directly to withdraw your consent for what they do with your personal data.

To comply with payment services regulations, we have to share some of your personal data with other payment service providers in some circumstances such as when you ask us to share information about your account with them. Whilst those payment services regulations mention 'consent' for this, 'consent' in that context does not have the same meaning as 'consent' under data protection laws. The legal grounds which may be relevant to this are compliance with our legal obligations, performance of our contract with you, our legitimate interests, or a combination of these. This is why if you ask to revoke consent with respect to what we do with your personal data, we may still have to hold and use that personal data if we need to under the payment services regulations.

10. Who might we share your data with?

In order to provide our services, there will be times when we will share your data. These include:

Sharing with other parts of Aldermore Bank

Aldermore Group is a member of the First Rand Group of Companies.

In order to provide our services as necessary, there will be times when we may need to share your data. We may share your personal information with these organisations:

- Members of the FirstRand Group
- Aldermore Group entities, including Motonovo Finance

'FirstRand limited' and its various members make up 'FirstRand Group'. For more information about how data is used at FirstRand please see group-customer-privacy-notice-2023.pdf

'Aldermore Group' includes Aldermore Bank Plc and Motonovo Finance Ltd. For more information about how data is used at Motonovo Finance ltd, please see **https://customer.motonovofinance.com/privacy**

Sharing with our contracted third-party suppliers

We may share your personal data with companies whom we have contracts in place for the supply of goods and services as part of providing service to our customers, such as our mailing house and website suppliers.

We may also disclose your personal data to our appointed representatives in connection with a contracted transaction between you and us. This includes solicitors, surveyors, valuers, insurers, loss adjusters and any party described in the terms and conditions of the individual products you hold with us. We will have in place an agreement with our service providers which will restrict how they are able to process your personal data. If any service provider is based outside of the European Economic Area, we will ensure that the provider is either a current subscriber to the EU/US Privacy Shield, or we have an appropriate contract for the international transfer of personal data with them.

We may share your personal information with these organisations:

- Agents and advisers who we use to help run your accounts and services, collect what you owe, and explore new ways of doing business
- HM Revenue & Customs, regulators and other authorities
- UK Financial Services Compensation Scheme
- Credit Reference Agencies
- Fraud Prevention Agencies
- Any party linked with you or your business's product or service
- Companies we have a joint venture or agreement to co-operate with
- Organisations that introduce you to us
- Companies that we introduce you to
- Market researchers
- Price comparison websites and similar companies that offer ways to research and apply for financial products and services
- Companies you ask us to share your data with
- Confirmation of Payee (CoP) service providers

We may need to share your personal information with other organisations to provide you with the product or service you have chosen:

- If you use direct debits, we will share your data with the Direct Debit scheme
- 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
- To ensure the bank details that you have provided match account details of the Sort Code and Account Number, we will use a third-party Confirmation of Payee (CoP) service provider.

Sharing where we are obliged under a legal obligation

We will disclose your personal data in order to comply with any legal regulations or good governance obligations, or to enforce or to protect our rights, property, or safety, or that of our customers or other persons with whom we have a business relationship. This includes exchanging information (which may include information relating to debts which are owed to you, and the related debtors) with other companies and organisations for the purposes of fraud protection, credit insurance and credit risk reduction.

Sharing information with Credit Reference Agencies

To process your application, we will perform credit and identity checks on you with one or more Credit Reference Agencies ("CRAs"). Where you take products or services from us, we may also make periodic searches (up to annually) at CRAs to manage your account with us.

To do this, we will supply your personal data to CRAs and they will give us information about you. This will include information from your credit application and about your financial situation and financial history. CRAs will supply to us both public (including the electoral register) and shared credit, financial situation and financial history information and fraud prevention information.

We will use this information to:

- Assess your creditworthiness and whether you can afford to take the product
- Verify the accuracy of the data you have provided to us
- Prevent criminal activity, fraud and money laundering
- Manage your account(s)
- Trace and recover debts, and
- Ensure any offers provided to you are appropriate to your circumstances

We will continue to exchange information about you with CRAs while you have a relationship with us. We will also inform the CRAs about your settled accounts. If you borrow and do not repay in full and on time, CRAs will record the outstanding debt. This information may be supplied to other organisations by CRAs.

When CRAs receive a search from us they may place a search footprint on your credit file that may be seen by other lenders. There are two types of searches 'soft credit checks' which has no footprint on your credit file. The other type of search is a 'hard credit check' which will leave a record of a credit file. Too many hard credit checks in a short period of time can affect your credit score for six months. This may reduce your chances of getting credit at Aldermore or another provider.

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

If you are making an application on behalf of a business or corporate entity credit checks may take place on company directors, beneficial owners and other people associated with the company such as guarantors at the pre-application, application stage, and periodically after that (up to annually).

The identities of the CRAs, their role also as Fraud Prevention Agencies, the data they hold, the ways in which they use and share personal data, data retention periods and your data protection rights with the CRAs are explained in more detail at **https://www.experian.co.uk/legal/crain/**

The CRAs also collect and use personal data for marketing and data profiling activities, to create data modelling tools. These tools are used to model customer behaviour to support marketing, research, brand and product communication campaigns.

You can find out more about how CRAs use your data and how you can opt out at **www.experian.co.uk/privacy/consumer-information-portal/**

TransUnion shall process such personal data in accordance with the notice displayed on the TransUnion Website, at **https://www.transunion.co.uk/legal/privacy-centre** or such URL as is notified to the Client from time to time. The Client agrees to make the notice available to the Client Users in an appropriate manner so they are aware of TransUnion's processing of such data.

Equifax shall process such personal data in accordance with the notice displayed on the Equifax Website, at **https://www.equifax.co.uk/About-us/Privacy_policy.html**

Sharing information with Fraud Prevention Agencies (FPAs)

Before we provide services, goods or financing to you, we undertake checks for the purposes of preventing fraud and money laundering, and to verify your identity. These checks require us to process personal data about you.

What we process and share

The personal data you have provided, we have collected from you, or we have received from third parties may include your:

- name
- date of birth
- residential address and address history
- contact details such as email address and telephone numbers
- financial information
- employment details
- identifiers assigned to your computer or other internet connected device including your Internet Protocol (IP) address
- vehicle details

When we and Fraud Prevention Agencies process your personal data, we do so on the basis that we have a legitimate interest in preventing fraud and money laundering, and to verify identity, in order to protect our business and to comply with laws that apply to us. Such processing is also a contractual requirement of the services or financing you have requested.

We, and 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 decisions

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

- our processing reveals your behaviour to be consistent with that of known fraudsters or money launderers; or is inconsistent with your previous submissions; or
- you appear to have deliberately hidden your true identity.

You have rights in relation to automated decision making: if you want to know more please contact us by any of the means listed in the Contact us section of our website.

Sharing under change of business ownership

In the event that we sell or buy any business or assets, we may disclose your personal data to the prospective seller or buyer of such business or assets.

If Aldermore or substantially all of its assets are acquired by a third party, the personal data we hold about our customers will be one of the transferred assets.

Market researchers

Aldermore Bank may contact you via email to invite you to review any services and/or products you received from us [in order to collect your feedback and improve our services [and products]] (the "Purpose"). We use an external company, Trustpilot A/S ("Trustpilot"), to collect your feedback which means that we will share your name, email address and reference number with Trustpilot for the Purpose. If you want to read more about how Trustpilot process your data, you can find their Privacy Policy **https://legal.trustpilot.com/for-reviewers/end-user-privacy-terms**

Aldermore Bank may also use such reviews in other promotional material and media for our advertising and promotional purposes.

11. Transferring Data Abroad

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

- Follow your instructions
- Comply with a legal or regulatory duty
- On rare occasions, where this is required by suppliers who help run your accounts and services (such as cloud hosted services).
- Information we may need to share with our parent company First Rand for legal, regulatory or financial management purposes.

Should we need to transfer your data outside of the EEA for any reason, we will ensure that there are safeguard in place. Safeguards include contractual obligations imposed on the recipients of your personal data. Those obligations require the recipient to protect your personal data to the standard required in the EEA. For further information, please visit the European Commission Justice Webpage (**https://ec.europa.eu/info/law/law-topic/data-protection_en**)

Safeguards also include requiring the recipient to subscribe to 'international frameworks' intended to enable secure data sharing and where the framework is the means of protection for the personal data.

Fraud prevention agencies may allow the transfer of your personal data outside of the UK. This may be to a country where the UK Government has decided that your data will be protected to UK standards, but if the transfer is to another type of country, then the fraud prevention agencies will ensure your data continues to be protected by ensuring appropriate safeguards are in place. Please note National Hunter rules currently do not allow for processing National Hunter data outside of the UK and European Economic area.

If it is necessary to transfer your personal data to the United States of America (US) as part of a service, we may use the UK-US data bridge to confirm adequacy arrangements. The data bridge provides assurances that organisations have appropriate and effective controls in place for the management and protection of personal data. Further information on the UK-US Data Bridge can be found on the **UK government website**.

12. What should you do if your personal data changes?

You should tell us without delay so that we can update our records. If you were introduced to us by a broker or other intermediary who is Data Controller in its own right, you should contact them separately. In some cases where you exercise rights against us under data protection laws (see below) we may need to inform the broker or other intermediary, but this will not always be the case.

13. Do you have to provide your personal data to us?

We are unable to provide you with a product or service or to process your application without having personal data about you. Your personal data is required before you can enter into the relevant contract with us, or it is required during the life of that contract, or it is required by laws that apply to us. If we already hold some of the personal data that we need – for instance if you are already a customer – we may not need to collect it again when you make your application. In all other cases we will need to collect it except as follows:

In cases where providing some personal data is optional, we will make this clear. For instance, we will say in application forms or on our website or via the broker or other intermediary if alternative (such as work) telephone number contact details can be left blank.

14. How long we keep your information

Your data is important to us and we take all reasonable steps to maintain it safely and securely and fully in accordance with the UK Data Protection Act 2018.

We will keep your personal data for up to seven years from end of last financial year of our business relationship with you. This includes credit agreements, applications forms (paper and electronic), ID provided, credit scores, payments default records and complaints.

After this time, the data is securely disposed of.

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.

Personal data may be held for a longer period due to business continuity and backup procedures. This can be up to 10 years, and is in line with ICO guidance on retention of data which has been backed up (See section 23 for further details.) This information is not accessible on Aldermore systems and will not be used for any other purpose.

15. Marketing

Personal customers

Personal customers means individuals, sole traders and partnerships.

Unless you don't want us to, we'll keep you informed about our products and services that are similar to those you already have.

If you are a sole trader or partnership we'd love to send you information about supporting a business and managing employees. This information will be sent from us about our partner companies. It's entirely up to you if you want to receive this. You're in control. We'll ask you to opt in to receive this information.

Business customers

In our terms and conditions, business customers means limited and public limited companies.

Unless you don't want us to, we'll keep you informed about our products and services that are similar to those you already have.

We'd love to send you information about supporting a business and managing employees. This information will be sent from us about our partner companies. It's entirely up to you if you want to receive this.

You're in control. You can opt-out of these at any time.

All customers: how to stop receiving marketing communications

If you don't want marketing communications from us anymore, you can opt out at any time. You can let us know by following the instructions included in the marketing communication you've received. Or, you can go to your account, if you have one, or go to our contact us page on our website.

Alternatively, you can tell our **data protection officer**.

16. Your Rights

Here is a list of the rights that all individuals have under data protection laws. They do not apply in all circumstances. If you wish to exercise any of them we will explain at that time if they are engaged or not.

The **right to be informed** - we must be transparent with you about the processing that we do with your personal data. This is why we have a privacy policy. The information that you supply is determined by whether we collected your personal data directly from you or indirectly via someone else (such as a broker or other intermediary). Your right to be informed may be relevant if you consider it necessary to ask for more information about what we do with your personal data.

The **right to request access** to the personal data held about you, to obtain confirmation that it is being processed, and to obtain certain prescribed information about how we process it. This may assist if you wish to find out what personal data we do have about you to then determine if you can exercise other rights (those mentioned above and below).

You can exercise this right by contacting us or submitting our Data Subject Rights Request form at **https://www.aldermore.co.uk/dsar**. Submitting the from will help us to locate your data quickly and provide it to you in good time.

The **right to object** to processing of your personal data where it is based on legitimate interests, where it is processed for direct marketing (including profiling relevant to direct marketing) or where it is processed for the purposes of statistics. Your rights to object may be relevant if you wish to find out more about what legitimate interests we rely on (they are listed in our privacy policy) or about what profiling we do in relation to our direct marketing communications and activities (as mentioned in our privacy policy) for instance. There is an important difference between the right to object to profiling relevant to direct marketing in cases where that profiling activity does not have a legal effect on you or otherwise significantly affect you, and the separate right which exists under data protection laws in relation to profiling including automated decision making which has a legal effect or can otherwise significantly affect you (see below).

The **right to restrict processing** of your personal data, for instance where you contest it as being inaccurate (until the accuracy is verified); where you have objected to the processing (where it was necessary for legitimate interests) and we are considering whether our organisation's legitimate interests override your own; where you consider that the processing is unlawful (and where this is the case) and where you oppose erasure and request restriction instead; or where we no longer need the personal data for the purposes of the processing for which we were holding it but where you require us to continue to hold it for the establishment, exercise or defence of legal claims.

The **right to have your personal data erased** (also known as the "right to be forgotten"). This enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This right is not absolute – it applies only in particular circumstances and where it does not apply any request for erasure will be rejected. It may be relevant 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 then withdraw; when you object to the processing and there is no overriding legitimate interest for continuing it; 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 may be refused in some circumstances such as where the personal data must be retained to comply with a legal obligation or to exercise or defend legal claims.

The **right to have your personal data corrected if it is inaccurate** and to have **incomplete personal data completed** in certain circumstances. If we have disclosed the personal data in question to other organisations, we must inform them of the rectification where possible. Your rights in relation to rectification may be relevant if you consider that we are processing inaccurate or incomplete information about you.

The **right to data portability**. This allows individuals to obtain and reuse their personal data for their own purposes across different services; to move, copy or transfer their personal data easily from one environment to another in a safe and secure way without hindrance to usability. This right can only be relevant where personal data is being processed based on a consent or for performance of a contract and is carried out by automated means. This right is different from the right of access (see above) and that the types of information you can obtain under the 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 automated decision making which has a legal effect or otherwise significantly affects you. This right allows individuals in certain circumstances to access certain safeguards against the risk that a potentially damaging decision is taken solely without human intervention. This right is different from the more general right to object to profiling (see above) because that other right is not tied to a scenario where there is a legal effect on you or where the processing otherwise significant affects you. Data protection laws prohibit this particular type of automated decision making except where it is necessary for entering into or performing a contract; is authorised by law; or where you have explicitly consented to it. In those cases, you have the right to obtain human intervention and an explanation of the decision and you may be able to challenge that decision.

You also have a **right to complain** to the Information Commissioner's Office (ICO website) which regulates the processing of personal data in the UK.

If you wish to find out more about your data subject rights or how to exercise them, please contact our Data Protection Officer using the contact information below.

If you wish to exercise any of these rights against the Credit Reference Agencies, the Fraud Prevention Agencies, or a broker or other intermediary who is Data Controller in its own right, you should contact them separately.

17. Do we do any monitoring involving processing of your personal data?

In this section monitoring means any listening to, recording of, viewing of, intercepting of, or taking and keeping records (as the case may be) of calls, emails, text messages, instant messages, social media messages, face-to-face meetings and other communications.

We may monitor where permitted by law and we will do this where the law requires it. In particular, where we are required by the Financial Conduct Authority's regulatory regime to record certain telephone calls or in person meetings we will do so.

Some of our monitoring may be to comply with regulatory rules, self- regulatory practices or procedures relevant to our business, to prevent or detect crime, in the interests of protecting the security of our communications systems and procedures, to have a record of what we have discussed with you and actions agreed with you, to protect you and to provide security for you (such as in relation to fraud risks of your account) and for quality control and staff training purposes.

We may conduct short term carefully controlled monitoring of your activities on your account where this is necessary for our legitimate interests or to comply with our legal obligations. For instance, where we suspect fraud, money laundering or other crimes.

Telephone calls and/or in person meetings between us and you in connection with your application and the product or service may be recorded to make sure that we have a record of what has been discussed and what your instructions are. We may also record these types of calls for quality control, compliance, complaint handling and staff training.

We may also record calls and/or interactive meetings or events using Conferencing tools, in such cases a notice or warning will be provided at the start of calls. We may record meetings to produce minutes and track actions.

Events, workshops or webinars may be recorded to make the content available on our intranet or website for the benefit of colleagues, partners and customers.

18. Use of Automated Processing and Automated Decision Making

Use of Automated Processing and Automated Decision Making

Like many Financial Service providers, we use automated processing in our account opening and identification processes. This means we attempt to match your personal details to publicly available information through sources such as the Royal Mail or Credit Reference Agencies. If for any reason we are unable to complete our formalities using this process you will be informed how you many complete the process using manual methods.

As part of the processing of your personal data, decisions may be made by automated means. This means we may automatically decide that you pose a fraud or money laundering risk or if our processing reveals your behaviour to be consistent with that of known fraudsters or money launderers; or is inconsistent with your previous submissions; or you appear to have deliberately hidden your true identity.

Here are some examples of the types of automated decisions we make:

Pricing

We may decide what to charge for some products and services based on what we know.

Tailoring products and services

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 and services for different customer segments, and to manage our relationships with them.

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 meets 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.

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. (details in the Contact us section at the bottom of this policy.

19. Consequences of Processing

If we, or a Fraud Prevention Agency, determine that you pose a fraud or money laundering risk, we may refuse to provide the services and products you have requested, or to employ you, or we may stop providing existing services to you.

A record of any fraud or money laundering risk will be retained by the Fraud Prevention Agencies, and may result in others refusing to provide services, financing or employment to you. If you have any questions about this, please contact us using the details provided.

20. Profiling

We use our customers' data to understand how our website is operating, to track how certain products are performing and to generate business strategy based on statistical analysis.

For this we profile using data generated throughout your contact with the Bank by our online applications and in strict accordance with the Bank's Cookie policy.

Profiling is also relied upon in the processes used by Credit Reference Agencies where automated decisioning methods are used to check for fraud or Money Laundering activity. You have rights in relation to auto decisioning so contact us if you want to learn more.

We also profile your data to help us identify opportunities for us to maximise the benefits to you of being an Aldermore customer, such as, for example, through the provision of special offers, unless you have told us that you do not want us to do this.

We can do this activity based on our legitimate interests (and they are listed in the 'What we do with your data' section above) only where the profiling and other automated decision making does not have a legal or other significant effect on you. In all other cases, we can do this activity only where it is necessary for entering into or performing the relevant contract, is authorised by laws that apply to us, or is based on your explicit consent. In those cases, you have the right to obtain human intervention to contest the decision (see 'rights in relation to automated decision making which has a legal effect or otherwise significantly affects you' above). Profiling for direct marketing can mean there is a separate right to object (see 'rights to object' above). If you want to know more, please contact us using the details provided.

21. Data Anonymisation and the use of Aggregated Information

Your personal data may be converted into statistical or aggregated data which cannot be used to re-identify you. It may then be used to produce statistical research and reports.

This aggregated data may be shared and used in all the ways described in this privacy policy.

22. Data Privacy Notices from Other Organisations

We have mentioned that we share your personal data with Fraud Prevention Agencies and Credit Reference Agencies. They require us to pass on to you information about how they will use your personal data to perform their services or functions as Data Controllers in their own right. These notices are separate to our own.

23. Useful Links

Aldermore cookie policy

aldermore.co.uk/legal/cookie-policy

More information about how Credit Reference Agencies operate and how they use your information is available at:

Credit Reference Agency Privacy Notices:

Experian
https://www.experian.co.uk/privacy

TransUnion
https://www.transunion.co.uk/legal/privacy-centre

Equifax
https://www.equifax.co.uk/About-us/Privacy_policy.html

Additional useful links

ICO website
https://ico.org.uk

ICO guidance for back up retention
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/right-to-erasure/#ib5

National Hunter
National Hunter,
PO Box 4744,
Stone,
ST159FE
nhunter.co.uk

Credit Industry Fraud Avoidance System
https://www.cifas.org.uk/fpn

24. Contact us

You can contact our Data Protection officer at the following address:

Data Protection Officer
Aldermore
4th Floor
40 Spring Gardens
Manchester
M2 1EN

Email: **DPO@aldermore.co.uk**

Aldermore

Aldermore documentation is available in Braille, large print and audio versions.

ASV0675-0525