AL RAYAN BANK

Welcome to Al Rayan Bank's Privacy Notice

Al Rayan Bank respects your privacy and is committed to protecting your personal data. This Privacy Notice informs you about how we use and look after your personal data, including any data you may provide through this website, or when you request information about other products or services from the bank or otherwise communicate with us, when we provide our products and services to you and when information and personal data is provided to us relating to our business. This Notice also informs you about your privacy rights and how the law protects you.

This Notice applies to any individual whose personal information we hold or use, whether you are a current or prospective customer or supplier or anyone else. Employees of the bank should, however, refer to the *the Employee Privacy Notice* which contains specific information for them.

Who we are

Al Rayan Bank PLC is the controller and responsible for your personal data (referred to as "Al Rayan Bank", the "Bank", "we", "us" or "our" in this Privacy Notice). Al Rayan Bank PLC is also responsible for this website.

Our Data Protection Officer is responsible for overseeing questions in relation to this Privacy Notice. If you have any questions about this Privacy Notice, including any requests to exercise your legal rights (including any opt-out mentioned in this Privacy Notice), please contact the Data Protection Officer using the details set out below.

Contact details

Our full details are:

- Name of legal entity: Al Rayan Bank PLC (No. 4483430) registered in England and Wales and authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.
- Email address of the Data Protection Officer: dataprotection@alrayanbank.co.uk
- Postal address of the Bank and the Data Protection Officer: PO Box 12461, Birmingham, B16 6AQ.
- Telephone number: 0800 408 6407

If you have a complaint relating to the use of your personal data, please contact the Data Protection Officer by email, telephone, or post at the above address. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues (https://ico.org.uk). We would, however, prefer to deal with your concerns before you approach the ICO, so please contact us in the first instance.

In this Privacy Notice, the terms "personal data", "processing", "data controller" and "data processor" shall have the meaning ascribed to them in the UK General Data Protection Regulation 2018 (UK GDPR).

Calling us

When you call us on 0800 408 6407, we collect Calling Line Identification (CLI) information. This is the phone number you are calling from (if it's not withheld). We hold a log of the phone number, date, time and duration of the call. We hold this information for 90 days. We use this information to understand the demand for our services and to improve how we operate. We may also use the number to call you back if you have asked us to do so, if your call drops, or if there is a problem with the line. We may also use it to check how many calls we have received from it. We audio record any calls, and we might make notes to help us answer your query. Other bank staff may also listen in during your call for training or quality assurance purposes.

Social media

We manage all messages and comments sent to us using social media channels and decide how we manage it. For example, if you send a message via social media that needs a response from us, we may process it in our case management system as an enquiry or a complaint. When contacting the bank through a social media platform, we suggest you also familiarise yourself with the privacy information of that platform. If you send us a private or direct message via social media, it will be stored by ourselves or by our third-party provider for three months.

Live chat

We use a third-party provider, LiveChat, to supply and support our live chat service. If you use our live chat service, we'll collect the contents of your live chat session and if you choose to provide it your name and email address. LiveChat retains this data for us for 90 days.

Emailing us

We use Transport Layer Security (TLS) to encrypt and protect email traffic in line with government guidance on email security. Most webmail such as Gmail and Hotmail use TLS by default. We'll also monitor any emails sent to us, including file attachments, for viruses or malicious software. All outgoing email is also scanned for compliance to company policy. You must ensure that any email you send is within the bounds of the law.

1. Personal data we collect

Most of our data comes directly from you, our customer, for example, when you apply for a product. This will include the following:

- personal details (e.g., name, date of birth, passport information or other identification information);
- contact details (e.g., phone number, email address, postal address or mobile number);
- transactional details (e.g., payments you make and receive);
- financial information (e.g., bank account number, credit or debit card numbers, financial history);
- details about your health (e.g., to meet our regulatory obligations, including responsible financing);
- religious beliefs (e.g., we may ask for information about these from you to help us decide whether to recommend Sharia compliant products that meet your financial needs (such as Home Purchase Plan) to you);
- information about criminal convictions and offences (e.g., for Home Purchase Plan applications); and
- information about any other Al Rayan Bank products and services you currently have, you have applied for, or you have previously held.

If you do not provide personal data that we request, it may mean that we are unable to provide you with the services and/or perform all of our obligations under our agreement with you.

We will also hold information we collect about you from other sources. This could include:

- the way you are using our branches, telephone services, websites or mobile applications;
- your interactions with us, for example through our branches, telephone services, websites, mobile applications, social media or other channels;
- the way you use your accounts, including information about payments you make or receive, including the details of the payee or payer (for example, retailers or other individuals);
- our parent company, which is based in Qatar, for example if they refer you to us;
- our own records about any other accounts or products you have with us or other providers;
- information from credit reference agencies and fraud prevention agencies;
- publicly available information about you which is available online or otherwise;
- organisations that provide their own data, or data from other third parties, to enable us to enhance the personal data we hold, and then provide more relevant and interesting products and services to you;
- criminal record checks and information;
- employers;
- joint account holders;
- people appointed to act on your behalf (such as independent financial advisers, accountants etc).

We also collect personal data automatically when you use the website and when you navigate through the website. Data collected automatically may include usage details, geo-location data, IP addresses and other data collected through cookies and other tracking technologies. For more information on our use of these technologies, see our Cookie Notice https://www.alrayanbank.co.uk/cookies-policy.

We may monitor or record phone calls with you in case we need to check we have carried out your instructions correctly, to resolve queries or issues, for regulatory purposes, to help improve our quality of service and to help detect or prevent fraud or other crimes. Conversations may also be monitored for staff training purposes.

We may also receive data from publicly availably sources such as Companies House and the Electoral Register.

If you give us personal data about other people, then you confirm that they are aware of the information in this Notice about how we will use their personal data. This may happen if you supply us information about your dependents or joint account holders.

If we collect personal information relating to children (under 13 years old) as part of their application for a savings account for example, or as a dependant of an applicant for a Home Purchase Plan, we ensure a parent or guardian is aware of the information being provided.

2. How we use your personal data, and the legal basis for doing so

We are can only process your personal data on a basis permitted by law. The legal basis will usually one of the following:

- to allow us to take actions that are necessary in order to provide you with the product/service (to perform our contract with you); for example, to make and receive payments;
- necessary to allow us to comply with our legal obligations; for example, obtaining proof of identity for anti-money laundering obligations;
- necessary for our or your legitimate interests; for example, to help us develop and improve our services;
- where we have your consent to do so; or
- in the case of special categories of personal data, that it is in the substantial public interest.

We have set out below, in a table format, a description of all the ways we use the various types of personal information and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate. Note that we may process your personal data on more than one lawful basis depending on the specific purpose for which we are using your data. Where we are relying on a legitimate interest, these are also set out below:

Purpose/Activity	**Lawful basis for processing including basis of legitimate interest**
To register you as a new customer.	Performance of a contract with you.
To provide, manage and personalise our services to you.	(a) Performance of a contract with you; (b) Necessary to comply with a legal obligation; (b) Necessary for our legitimate interests (to maintain standards of service, protect our business interests, provide an efficient service).
To manage our relationship with you which will include: (a) Notifying you about changes to our terms or Privacy Notice (b) Communicating with you about the product or service (c) To manage complaints, rectify problems and to resolve queries (d) Recording telephone calls.	(a) Performance of a contract with you; (b) Necessary to comply with a legal obligation; (c) Necessary for our legitimate interests (to keep our records updated, provide a high standard of service, to study how customers use our products/services, avoid complaints in future).

To develop and improve products and services through assessment and analysis of the information, including credit or behavioural scoring (or both), market and product analysis, and market research. Behavioural monitoring will focus on data points such as mouse activity, keystroke movement and touchscreen behaviour.	(a) Necessary to comply with a legal obligation; (b) Necessary for our legitimate interests (to study how customers use our products/services, to develop them and grow our business).
To manage our relationships with suppliers (using personal contact information they have provided); for example, to arrange servicing agreements; contacts and correspondence with suppliers; and to follow up invoice queries, issue escalations and resolutions in line with the agreed contractual terms and conditions. From time to time this supplier information may be used to invite supplier staff to meetings and events.	(a) Performance of a contract with you (the supplier); (b) Necessary for our legitimate interests (to maintain standards of service, run our business efficiently, protect our business interests).
To administer and protect our business and this website (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data).	(a) Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise); (b) Necessary to comply with a legal obligation.
To undertake checks for the purposes of security and for detecting and preventing fraud and money laundering, and to verify your identity before we provide services to you.	(a) Performance of a contract with you; (b) Necessary to comply with a legal obligation; (c) Necessary for our legitimate interests (to protect our business, prevent fraud, money-laundering and other crimes).
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences.	Necessary for our legitimate interests (to define types of customers/subscribers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy).
To recover any outstanding amounts that are due to us, but unpaid, and enforce other obligations we are entitled to under our agreement(s) with you and protect our business against harm to our rights and interests.	(a) Performance of a contract with you; (b) Necessary to comply with a legal obligation; (c) Necessary for our legitimate interests (to ensure that our business is run prudently, and we can recover any outstanding amounts that are due to us, but unpaid, as well as protecting our assets).

To verify your identity and the identity of joint account holders, for example by using caller line identification technology to check we are speaking to the correct person.	(a) Performance of a contract with you; (b) Necessary to comply with a legal obligation; (c) Necessary for our legitimate interests (to protect our business and comply with legal and regulatory obligations).
To comply with regulatory and legal obligations to which we are subject and cooperate with regulators and law enforcement bodies.	(a) Necessary to comply with a legal obligation; (b) Necessary for our legitimate interests (to protect our business); (c) For the use of sensitive data, where it is in the substantial public interest.
To make suggestions and recommendations to you about products or services that may be of interest to you (unless you have opted out of marketing), including personalising marketing messages.	(a) Necessary for our and your legitimate interests (to develop our products/services, provide products of interest to you and grow our business); (b) Where you are a personal customer, in relation to electronic marketing, where we have your consent to do so.

Special categories of data

Some of the information we collect are special categories of personal data (also known as sensitive personal data).

In particular, we may process personal data that relates to your health (such as medical history) (for example to determine if you are a vulnerable customer) and any criminal convictions and offences (for due diligence reasons). We may also obtain information about religious beliefs (we may ask for information about these from you to help us decide whether to recommend to you Sharia compliant products that meet your financial needs, such as Home Purchase Plan). We may encourage the use of biometric information (fingerprint, palmprint, voice and/or facial recognition) as a way of enhancing the security of, for example, your digital interactions with us or for the use of safe deposit boxes.

Where we process such special category data or criminal records, we will usually do so on the basis that it is necessary for reasons of substantial public interest, to establish, exercise or defend any legal claims, or in some cases, with explicit consent. In any case, we will carry out the processing in accordance with applicable laws.

What we use your special category data for	Lawful basis for processing
If you are a personal customer, for due diligence checks (e.g., criminal convictions).	Substantial public interest
We may use medical information to help provide, manage and personalise our services, to resolve complaints and queries and help you apply for suitable products and services.	(a) Substantial public interest; (b) Where we have your consent.
We may ask you for information which might allow us to know your religious beliefs, to help us decide whether to recommend to you Sharia compliant	Where we have your consent

products that meet your financial needs (such as Home Purchase Plan).	
In order to provide our customers with a platform that offers secure and strong customer authentication we utilise third party service providers to aid us in the ensuring verification of you and your transactions. We have been changing the way you authenticate, and this includes the option to utilise a behavioural biometric as a second factor to the One Time Passcode (OTP) option. This is achieved by recording the keystrokes of cardholders entering their OTP value into the 3D Secure dialogue box and it applies learning algorithms and statistical models to differentiate between a valid user and a fraudster, or BOT.	Where we have your consent
We may use medical information and criminal convictions data to temporarily postpone payments due to us and help us consider suitable payment plans.	Substantial public interest
To comply with regulatory and legal obligations to which we are subject and cooperate with regulators and law enforcement bodies.	Substantial public interest

We collect certain special categories of personal data about employees and prospective employees who should refer to the Al Rayan Bank Staff Privacy Notice.

Automated Decision Making

The way we analyse personal data in relation to our services may involve profiling, which is processing your personal data using software that is able to evaluate your personal aspects and predict risks or outcomes. We may also use profiling, or otherwise employ solely automated means, to make decisions about you that relate to:

- credit limit decisions;
- credit and affordability assessment checks to determine whether your application will be accepted;
- identify and verification checks;
- anti-money laundering and sanctions checks;
- transaction monitoring for fraud and other financial crime, to prevent you committing fraud, or becoming a victim of fraud; and
- screening of individuals who may be classed as “politically exposed”.

This is known as “automated decision-making” and is only permitted when we have a legal basis for this type of decision-making. We may make automated decisions about you:

- where such decisions are necessary for entering into a contract. For example, we may decide not to offer our services to you, or we may decide on the types of services that are suitable for you, or how much to charge you for our products based on your credit history and other financial information we have collected about you;
- where such decisions are required or authorised by law, for example for fraud prevention purposes; or
- where it is a reasonable way of complying with government regulation or guidance, such as our high-level obligation to treat customers fairly.

You have rights in relation to automated decision making, for example you can request that an automated decision is reviewed by a human being: if you want to know more, please contact us using the details set out in the Contact Us section at the beginning of this Privacy Notice.

3. Messages to you (including marketing)

We may send you messages (by telephone, post, text and email and other digital means) to help you manage your account, to comply with regulatory obligations (such as contract changes) and to keep you informed about features of the products and services you use (including those of others that may be of interest to you). Our lawful ground of processing your personal data to send you marketing communications is either your consent or our legitimate interests (namely to grow our business).

You can ask us to stop or start sending you marketing messages at any time by contacting us (see Contact Us at the beginning of this Privacy Notice) or by following the unsubscribe instructions in our marketing messages.

Under the Privacy and Electronic Communications Regulations, we may send you marketing communications from us if (i) you opened an account or asked for information from our services or (ii) you agreed to receive marketing communications and, in each case, you have not opted out of receiving such communications since. Under these regulations, if you are a limited company, we may send you marketing emails without your consent. However, you can still opt out of receiving marketing emails from us at any time.

Before we share your personal data with any third party for their own marketing purposes, we will get your express consent.

You can ask us or third parties to stop sending you marketing messages at any time by logging into the website and checking or unchecking relevant boxes to adjust your marketing preferences OR by following the opt-out links on any marketing message sent to you.

If you opt out of receiving marketing communications this opt-out does not apply to personal data provided as a result of other transactions, such as purchases, warranty registrations etc.

4. Consent

In certain circumstances we may need to request your consent to collect and use certain types of personal data when we are required to do so by law (for example, sometimes when we process special category data or when we place cookies or similar technologies on devices or browsers). If we ask for your consent to process your personal data, you have the right to object and you may withdraw your consent at any time by following the unsubscribe instructions in our communications with you or by contacting us using the details set out in the Contact Us section at the beginning of this Privacy Notice or, if in relation to cookies or similar, via the Cookie Policy on https://www.alrayanbank.co.uk/cookies-policy.

Should you not wish to provide your consent, any services directly related to this data may not be provided.

For some information we do not need to seek your consent to process it as it is part of the *performance of a contract*. When you open an account with the Bank, you enter a legal relationship with us. Data collected as part of this falls under what is classified as our legal obligation. Other information is processed as part of our due diligence checks, which is known as the *legitimate interest principle* relating to personal data processing.

5. Who we may share your data with

We will treat all your personal information as private and confidential (even when you are no longer a customer). We will not reveal your name, address, or any details of your relationship with us to anyone including other companies in our own group, other than in the following cases:

- our parent company in Qatar when it has referred you to us, to let them know the services we are providing. Where we do this, your personal information will not be used by them for the purpose of marketing without your express consent;
- our third-party service providers. These may include for example:
    - those we engage to host and maintain the website and IT systems (software suppliers etc);
    - analytics and search engine service providers that assist us in the improvement and optimisation of this website;
    - payment processing service providers, including strong customer authentication (SCA) providers and those supporting confirmation of payee (CoP);
    - those who print statements and marketing materials, and who make credit and debit cards;

    - those who assist us with or partner with us in marketing campaigns;
    - standby servicer for credit refinancing;
    - SMS/Telephony provider;
    - surveyors and similar professional services firms we use for example in connection with our Home Purchase Plan;
    - companies you have paid from your account if they request our help with a payment;
- Introducers of business to us (such as independent financial advisers and home finance brokers);
- Potential guarantors;
- Estate Agents;
- Auditors;
- Credit reference agencies (see below at *Section 6*);
- Your advisers (such as lawyers, accountants and other professional advisers) if you have asked them to represent you or have for example given them a Power of Attorney;
- Other financial institutions you ask us to contact (such as a bank you are switching from);
- Fraud prevention agencies (for example if you give us false information) to help them detect and prevent fraud and other crimes;
- Her Majesty's Revenues and Customs (HMRC) and other government agencies (for example to validate the income and other financial information you provide to us for Home Purchase Plan and other applications);
- Law enforcement bodies (including the police, immigration authorities), Courts of law or as otherwise required or authorised by law; and
- Regulators, trade associations or government bodies (including the Child Support Agency) for the purposes of resolving complaints or disputes both internally and externally or to comply with any investigation by one of those bodies. Details (consistent with what is said in this Privacy Notice) of how we use your personal information are also summarised in our Terms and Conditions for Consumer Banking (para 12) and in our Terms and Conditions for Business Banking (clause 14). These include:
    - Financial Conduct Authority (FCA)
    - Prudential Regulation Authority (PRA)
    - Pensions Regulator
    - Information Commissioner's Office (ICO)
    - Financial Services Compensation Scheme (FSCS).

We may also disclose personal data to third parties if we are under a duty to disclose or share personal data relating to you in order to comply with any legal obligation, or in order to enforce or apply our website Terms of Use https://www.alrayanbank.co.uk/legal/ and other agreements; or to protect the rights, property, or safety of us, our clients, or others. For example, we may be required by law or regulation to share information about your accounts with the UK or relevant tax authorities, either directly or via the local tax authority. The tax authority we share the information with could then share that information with other appropriate tax authorities.

Before we disclose personal data to a third party, we take steps to ensure that the third party will protect personal data in accordance with applicable privacy laws and in a manner consistent with this Notice. Third parties are required to restrict their use of this personal data to the purpose for which the data was provided.

Sometimes the third party will be outside the UK, in which case see Section 7 for more information.

6. Credit reference agencies

We perform credit and identity checks on you with one or more credit reference agencies and fraud prevention agencies. We will supply your personal data to the credit reference agencies and fraud prevention agencies, and they will provide us with information about you.

We will also continue to exchange information about you with credit reference agencies while you have a relationship with us. The credit reference agencies may in turn share your personal data with other organisations, which may be used by those organisations to make decisions about you. This may affect your ability to obtain credit.

We may also continue to collect information from credit reference agencies about you after your account is closed.

When you open any account with us, you provide us with your explicit permission to access, process and retain any information you make available to us for the purposes of providing payment services to you. This does not affect any rights and obligation you or we have under data protection legislation. You can withdraw this consent by closing your account. If you do this, we will stop using your data unless we have lawful grounds to do so. The agency that we approach will keep details of the type of search we request, even if your application with us does not proceed.

Other organisations may subsequently use the records and information held by the credit reference agency that we approach to carry out a credit search, including the details of a credit decision made about you or other persons associated with your application.

As well as using outside agencies to carry out credit and identity checks we will need to carry out our own credit checks to assess your applications for products or services with us or to check details relevant to your existing account with us. Where we do this, we may also use our own credit-scoring methods and carry out our own identity checks, including searching the Electoral Register.

We need to make these searches so that we obtain sufficient credit information to make a proper assessment of which of our products and services are most suited to your needs and to help verify your identity. Carrying out these searches enables us to open an account more quickly and helps to lessen the risk of fraud or other criminal activity taking place.

To help us form an accurate view of your existing financial commitments, searches made by us, or a credit reference agency, may “link” to the records of others that have entered into joint financial obligations with you (such as business partners and, if relevant, husbands, wives or other family members). Existing information held by credit reference agencies about you may be “linked” to other persons in this way. If so, you may be treated as financially “linked” for the purposes of any application you make to us, which means that you may be assessed in relation to joint obligations as well as those for which you are solely responsible.

If you apply for one of our products or services with another person or persons (for example in a joint account) you are declaring that you are entitled to disclose information about the other person or persons and authorise us to search, “link” or record information. Where we carry out a search through a credit reference agency a “link” will be created by the agency between you and the other person or persons. By making the application you and the other person or persons understand that each other’s information will be considered in future applications by any of you.

We may give details of the services and products that you have, and the way that you manage your account, to a credit reference agency. If you fail to comply with the conditions or the special conditions, we may tell a credit reference agency, and this may affect your ability to obtain financial services elsewhere.

Any of the information that we gather from a credit reference agency, or our own research may be used by us for the management of your account, identification purposes, debt tracing and the prevention of money laundering.

We will check your details with fraud prevention agency/agencies and if false or inaccurate information is provided and fraud is identified, details will be passed to fraud prevention agencies. Law enforcement agencies may access and use this information. We and other organisations also access and use this information to prevent fraud and money laundering.

Examples of circumstances when your information or information relating to your partner or other members of your household (or for business customers, their business partners) may be shared include:

- checking details provided on applications for products and services;
- making credit and affordability assessments and providing credit limits;
- managing credit and credit-related accounts or facilities;
- tracing your address so that we can continue to contact you about any existing or previous product(s) and account(s) you held with us, as well as recovering any outstanding amounts that are due to us, but unpaid;
- checking your identity to comply with regulations and the law;
- understanding your financial position through sharing and receiving information, for example about any financing (including financing outside Al Rayan Bank) and how you manage it. This includes the financial amount you obtain and your payment history; and
- in order to update or add personal data that is not included or incorrect in our records in order to meet our legal or regulatory obligations.

Please contact us on 0800 408 6407 if you want to receive details of the relevant fraud prevention agencies. We and other organisations may access and use from other countries the information recorded by fraud prevention agencies.

You have a right to access records held by a credit reference or fraud prevention agency. If you ask, we will tell you how to get a copy of the information that credit reference agencies have about you, or their leaflets that explain how credit referencing works. You should contact them directly and there may be a small charge for this. We are happy to provide contact details for such agencies on request.

Sometimes we may be approached by another person requesting that we provide a financial reference about you. If this happens, we will contact you and ask you to provide your written permission to do this.

We don't give information about savings accounts to credit reference agencies.

The Credit Reference Agency Information Notice (CRAIN) describes how the three main credit reference agencies in the UK each use and share personal data. The CRAIN is available on the credit reference agencies' websites:

- www.callcredit.co.uk/crain
- www.equifax.co.uk/crain
- www.experian.co.uk/crain

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.

7. Fraud Prevention Agencies (FPAs)

The personal information we've collected from you will be shared with fraud prevention agencies who will use it to:

- Prevent fraud;
- Prevent money-laundering; and
- Verify your identity.

If fraud is detected, you could be refused certain services, finance, or employment.

Further details on how your information will be used by us and these fraud prevention agencies, and your data protection rights, can be found by following the links below:

- CIFAS

We'll continue to exchange information about you with FPAs while you have a relationship with us.

We'll use this information to:

- Check the accuracy of the data you have provided to us;
- Prevent criminal activity, fraud, and money laundering; and
- Manage your account(s).

8. External links and social media sites

Although the website only looks to include safe and relevant external links, users should always adopt a note of caution before clicking any external web links mentioned throughout the website.

If you follow a link to any of these websites, please note that these websites have their own privacy policies or notices and that we do not accept any responsibility or liability for these policies. Please check these policies or notices before you submit any personal data to these websites.

Communication, engagement, and actions taken through external social media platforms are subject to the terms and conditions as well as the privacy policies of those social media platforms.

This website may use social sharing buttons which help share web content directly from our web pages to the social media platform in question. Where you use such social sharing buttons you do so at your own discretion. You should note that the social media platform may track and save your request to share a web page respectively through your social media platform account. Please note these social media platforms have their own privacy policies, and we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these social media platforms.

9. Where we store personal data

If you live outside the UK, the personal data relating to you that we collect may be transferred to, and stored at, locations outside our jurisdiction. It may also be processed by staff operating outside the UK who work for us or for one of our service providers.

As described in this Privacy Notice, we may also share personal data relating to you with third parties who are located overseas, for business purposes and operational, support and continuity purposes, for example, when we use IT service providers or data storage services.

Countries where personal data relating to you may be stored and/or processed, or where recipients of personal data relating to you may be located, may have data protection laws which differ to the data protection laws in your country of residence. By submitting your personal data, you accept that personal data relating to you may be transferred, stored or processed in this way.

We take measures to ensure that any international transfer of information is managed carefully and in accordance with data protection law to protect your rights and interests and in accordance with this Notice.

These measures include:

- Transfers of your personal data to countries which are recognised as providing an adequate level of legal protection for personal data;
- We have obtained the consent of data subjects to the international transfer of their personal data;
- Transfers within the Masraf Al Rayan (MAR) group where we have entered into an intra-group agreement, providing specific contractual protections designed to ensure that your personal data receives an adequate and consistent level of protection wherever it is transferred within the group;
- Transfers to organisations where we are satisfied about their data privacy and security standards and protected by contractual commitments such as signing a Data Processing Agreement and, where available, further assurances such as certification schemes; and
- The transfer will be to organisations that are part of the Privacy Shield if transferred to the United States of America.

If none of the above safeguards are available, we may request your explicit consent to the specific transfer. You will have the right to withdraw this consent at any time.

- if transferred to the United States of America, the transfer will be to organisations that are part of the Privacy Shield.

You have the right to ask us for more information about our safeguards. Please contact the Data Protection Officer (see the Contact Us section at the beginning of this Privacy Notice).

10. Changes of Business Ownership and Control

We may, from time to time, expand, reduce, or sell our business, and this may involve the transfer of certain divisions or the whole business to other parties. Personal data relating to you will, where it is relevant to any division so transferred, be transferred along with that division and the new owner or newly controlling party will, under the terms of this Privacy Notice, be permitted to use personal data relating to you for the purposes for which it was supplied by you.

11. How we keep your data safe

11a Security

Unfortunately, the transmission of information and data via the internet is not completely secure. Although we will do our best to protect personal data relating to you, we cannot guarantee the security of such data transmitted to the website; any transmission is at your own risk. Once we have received personal data relating to you, we use strict procedures and security features to try to prevent unauthorised access. The security of personal data regarding you is a high priority. We take such steps as are reasonable securely to store personal data regarding you so that it is protected from unauthorised use or access, misuse, loss, modification, or unauthorised disclosure. This includes both physical and electronic security measures. Examples include the use of passwords, locked storage cabinets and secured storage rooms. Other features include:

- storing information on secured networks consistent with industry standards, which are only accessible by those employees who have special access rights to such systems;
- using industry-standard encryption technologies when transferring or receiving personal data, such as SSL technology;
- restrictions are placed on the electronic transfer of files;
- our IT networks undergo regular necessary vulnerability testing to identify and remedy potential opportunities for unauthorised data access; and
- robust management of boundary firewalls, access controls, malware protection and patch release processes towards protecting customer data.

We have procedures in place to deal with any suspected personal data breach and will notify you and any

applicable regulator of a breach if we are legally required to.

11b Retaining your data

We will keep your personal data for as long as we have a relationship with you. Once our relationship with you has come to an end (e.g., following closure of your account or following a transaction), or your application for a product is declined or you decide not to go ahead with it, we will only retain your personal data for a period of time that is calculated depending on the type of personal data, and the purposes for which we hold that information.

When deciding what the correct time is to keep the data for, we look at its amount, nature and sensitivity, potential risk of harm from unauthorised use or disclosure, the processing purposes, if these can be achieved by other means and legal requirements.

For tax purposes the law requires us to keep basic information about our customers (including Contact, Identity, Financial and Transaction Data) for six years after they stop being customers.

In some circumstances we may anonymise your personal data for research or statistical purposes in which case we may use this information indefinitely without further notice to you.

We will only retain information that enables us to:

- maintain business records for analysis and/or audit purposes;
- defend or bring any existing or potential legal claims;
- maintain records of anyone who does not want to receive marketing from us;
- deal with any future complaints regarding the services we have delivered;
- assist with fraud monitoring;
- assess the effectiveness of marketing that we may have sent you; or
- comply with record retention requirements under the law (for example, as required under legislation concerning the prevention, detection and investigation of money laundering and terrorist financing).

We have a retention policy which helps us ensure information is only held for the correct period. We then delete or de-identify your data. The retention period is generally linked to the amount of time available to bring a legal claim, which in many cases is six- or seven-years following closure of your account or following a transaction. We will retain your personal data after this time if we are required to do so to comply with the law, if there are outstanding claims or complaints that will reasonably require your personal data to be retained, or for regulatory or technical reasons. If we do, we will continue to make sure your privacy is protected.

Note: for dormant accounts, these are kept for 15 years, in accordance with industry practice.

12. Your rights

You have certain rights regarding your personal data. These include the rights to:

- request a copy of the personal data we hold about you;
- request that we supply you (or a nominated third party) with an electronic copy of the personal data that you have provided us with;
- inform us of a correction to your personal data;
- exercise your right to restrict our use of your personal data;
- exercise your right to erase your personal data; or
- object to particular ways in which we are using your personal data (such as automated decision making, or profiling (for example to help us decide what products and services would suit you best); or
- understand the basis of international transfers of your data by us.

Where we rely on our legitimate interests to obtain and use your personal data then you have the right to object if you believe your fundamental rights and freedoms outweigh our legitimate interests. Where processing is carried out based upon your consent, you have the right to withdraw that consent.

Your ability to exercise these rights will depend on a number of factors and in some instances, we will not be able to comply with your request e.g., because we have legitimate grounds for not doing so or where the right does not apply to the particular data we hold on you.

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to

ask you for further information in relation to your request to speed up our response.

We ask that you contact us to update or correct your information if it changes or if the personal data we hold about you is inaccurate.

To exercise any of these rights and submit a Data Subject Access Request (DSAR), please contact the Data Protection Officer [email dataprotection@alrayanbank.co.uk] if you wish to exercise any of your rights.

If you have a concern about the way we are collecting or using personal data relating to you, we request that you raise your concern with us in the first instance. Alternatively, you can contact the Information Commissioner's Office at https://ico.org.uk/make-a-complaint/.

13. Changes to this Notice

We monitor and regularly update our policies and procedures to maintain the privacy of your personal information. As a result, our privacy notice may change from time to time. Any changes we make to this Notice in the future will be posted on this page and, where appropriate, notified to you by email. Please check back frequently to see any updates or changes to this Notice. The new terms may be displayed on-screen, and you may be required to read and accept them to continue your use of the website.

Last updated: March 2022