

Privacy Policy

Introduction

The privacy of your Personal Data is important to Alrajhi Bank. We are committed to protecting your information and ensuring transparency in how it is collected, used, stored and protected, in line with the Kingdom of Saudi Arabia's Personal Data Protection Law (PDPL) and its Implementing Regulations (together, the "PDPL"), and the requirements of the Saudi Central Bank (SAMA), including applicable rules, guidance and circulars issued by competent authorities from time to time.

This Policy is intended to provide you with clear and transparent information about how we collect, use, protect and otherwise process your Personal Data in accordance with applicable law.

This Policy explains the types of Personal Data we collect, the purposes for which it is used, and the measures we take to protect it. It also outlines your rights in relation to your Personal Data and how you can contact us or exercise those rights.

Who are we?

References in this Policy to "**Alrajhi Bank**", "**ARB**", "**we**", "**us**" and "**our**" include Alrajhi Bank (Commercial Registration No. 1010000096, with its registered address at 8467 King Fahad Road, Al Murooj District, Unit Number 1, Riyadh 12263 – 2743 Kingdom of Saudi Arabia) and its affiliates and subsidiaries, which are listed at the end of this document. We refer to these entities collectively as the "**ARB Group**".

In most cases, Alrajhi Bank acts as the controller in relation to your Personal Data because it determines why and how your Personal Data is processed. In some cases, ARB Group entities may process Personal Data on behalf of one another in accordance with applicable law. To know which entity is acting as a controller for the processing of your Personal Data, please go to page 14.

Who does this Policy apply to?

This Policy applies to you as a user of the Alrajhi Bank mobile application or our digital services. It also applies to individuals who interact with us through the application or in connection with products and services made available through it.

Where relevant, this may include individuals connected to you, such as authorised representatives, guarantors, beneficiaries or other related parties, to the extent their Personal Data is processed through the application.

We refer to each of these individuals as "**you**" or "**your**" in this Policy.

This Policy may be supplemented with additional product or service specific notices, or with additional information that governs our relationship with you. You should read this Policy alongside any such notices or information provided to you through the application or otherwise.

If you need help understanding which documents apply to you, please contact us using the details set out in the "How do you contact us?" section of this Policy.

What do we mean by Personal Data and Sensitive Personal Data?

When we refer to "**Personal Data**" in this Policy, we mean any information that identifies you, or that may directly or indirectly identify you, in accordance with the PDPL. This may include, for example, your name, identification number, address, contact details, account or card information, photographs and videos.

When we refer to "**Sensitive Data**" in this Policy, we mean a category of Personal Data that is considered particularly sensitive under the PDPL. This includes, for example, data revealing racial or ethnic origin, religious, intellectual or political beliefs, security or criminal data, biometric or genetic data, health data, or any other data classified as sensitive under applicable law.

What Personal Data do we collect?

We collect Personal Data about you as permitted by applicable law in connection with your use of the application and our digital services. The type and amount of Personal Data we collect will depend on the nature of your relationship with us and the products or services you access through the application.

We may collect the following categories of Personal Data:

1. **Personal and contact details:** Such as your name, date and place of birth, gender, nationality, identification details, telephone number, email address, postal address and communication preferences.
2. **Identification and verification information:** Such as copies of identification documents (e.g. national ID or passport), signatures, photographs, and other information used to verify your identity, which may include biometric data (such as facial images), where required for identity verification or security purposes and in accordance with applicable law.
3. **Financial and transaction information:** Including details of your accounts, card information, payment records, transaction history, income, savings, investments, sources of wealth and other financial activities.
4. **Account and relationship information:** Including information about the products and services you hold with us, documents you provide, and records of our interactions with you, including advice or support provided.
5. **Technical and usage information:** Such as IP address, login details, device information, browser type and settings, and information about how you use our websites, mobile applications and other digital services.
6. **Location information:** Such as information about the branches or cash machines you use, or general geographic location data derived from your interactions with us.

7. **Due diligence and compliance information:** Including credit data (where permitted), credit history, financial crime risk assessments, sanctions and anti-money laundering checks, fraud prevention data, and other information required to meet legal and regulatory obligations.
8. **Communications and customer support data:** Including call recordings, messages, emails, application forms, complaints, feedback, survey responses, and records of any communications between you and us.
9. **Marketing and preference information:** Including your preferences for receiving marketing communications, your participation in promotions or loyalty programmes, and your communication preferences.
10. **Social and publicly available information:** Such as information you share when interacting with us on social media, or information obtained from publicly available sources where permitted by law.
11. **Tax or regulatory information:** Including Zakat or other tax-related data where required to comply with legal or regulatory obligations.

Where relevant to specific products or services, we may also collect additional information, such as:

- **Insurance-related information**, including policy details and claims history
- **Health or medical information**, where required and with your consent
- **Information about individuals connected to you**, such as authorised representatives, guarantors or beneficiaries
- **Lifestyle or risk-related information**, where relevant to certain products (e.g. insurance)

We collect and use your Personal Data for the purposes described in the “How and why we use your Personal Data” section of this Policy.

Certain Personal Data is required for us to provide our services, comply with applicable legal and regulatory requirements, and manage our relationship with you. If you do not provide the required information, we may not be able to provide you with the relevant products or services or continue to provide them.

How we collect your Personal Data

We collect most of your Personal Data directly from you through your use of the application or when you interact with us through digital channels.

We collect Personal Data when you:

- register for or use the application
- apply for or manage products or services through the application
- communicate or interact with us through in-app features or digital channels
- participate in surveys, feedback or market research activities

We collect this information in order to establish and manage our relationship with you, including assessing your eligibility for products and services, providing those services, and managing your accounts and transactions.

We may also collect Personal Data from other sources where permitted by law, including:

- public sources and government authorities
- credit reference and fraud prevention agencies
- ARB Group entities
- third parties providing services to you
- social media platforms, where you interact with us or link your accounts
- authorised representatives and connected parties
- law enforcement or regulatory authorities
- government platforms, public registers and authorised service providers used for identity verification, credit assessment, address verification or compliance purposes
- credit bureaus and authorised platforms used for onboarding, verification, authentication, fraud prevention or regulatory compliance purposes

We may also use cookies and similar technologies in connection with your use of our digital services. Further details are set out in the “Cookies” section of this Policy.

Please note that providing certain Personal Data may be necessary for us to provide our products and services. If you do not provide the required information, this may affect our ability to deliver those services.

How and why do we use your Personal Data?

Under the Kingdom of Saudi Arabia’s Personal Data Protection Law (PDPL), we may only process your Personal Data where we have a valid legal basis to do so. Depending on the circumstances, this may include:

1. Contractual basis – where processing is necessary to enter into or perform a contract with you
2. Legal or regulatory obligation – where we are required to process Personal Data to comply with applicable laws or regulatory requirements, including those issued by the Saudi Central Bank (SAMA)
3. Legitimate interests – to the extent permitted under applicable law, where processing is necessary for our legitimate business interests and does not override your rights or involve Sensitive Data. Examples of our legitimate interests may include improving our products and services, supporting customer service, protecting our systems and networks, preventing fraud, and safeguarding our legal rights and business interests, in each case to the extent permitted under applicable law.
4. Consent – where you have provided your explicit consent
5. Actual interest – where processing is necessary to achieve a clear benefit for you and communication with you is impossible or difficult, in accordance with applicable law

We use your Personal Data for the purposes set out below. Depending on the specific product or service, not all categories of Personal Data will be processed for each purpose.

Purpose	Categories of Personal Data	Legal basis
Client onboarding and account opening , including identity verification, due diligence, eligibility assessment and regulatory checks	Personal identification details, contact details, employment and professional information, financial information, internal identifiers, due diligence and compliance data	Contractual basis, legal obligation, legitimate interests (to the extent permitted under applicable law)
Provision and management of banking products and services , including account operation, transactions, service delivery and access to digital platforms (including issuing access credentials)	Personal identification details, contact details, financial and transaction data, account information, digital activity	Contractual basis, legitimate interests
Sharing Personal Data with third parties to provide services , including ARB Group entities, payment providers, financial institutions, service providers and intermediaries	Personal identification details, financial data, transaction data, account information	Contractual basis, legal obligation, legitimate interests (to the extent permitted under applicable law)
Client relationship management , including customer service, communications, support, engagement and maintaining ongoing relationships	Personal identification details, contact details, communication records, digital activity, usage data, financial information	Contractual basis, legitimate interests (to the extent permitted under applicable law), consent (where applicable)
Creditworthiness assessment and credit checks , including fraud prevention agency and credit bureau checks	Personal identification details, contact details, financial information, credit data, internal identifiers	Contractual basis, consent (where required), legitimate interests (to the extent permitted under applicable law)
Compliance with legal and regulatory obligations , including SAMA requirements, AML, KYC, sanctions screening, reporting and regulatory investigations	Personal identification details, financial data, transaction data, communication records, due diligence data, sensitive data (where required)	Legal obligation
Risk management, fraud detection and prevention of financial crime , including monitoring transactions, preventing misuse of services and protecting customers and the Bank	Personal identification details, financial data, transaction data, technical data, usage data, communication records	Legal obligation, legitimate interests (to the extent permitted under applicable law)

Purpose	Categories of Personal Data	Legal basis
Security and systems protection , including preventing unauthorised access, ensuring IT security and protecting infrastructure	Technical data, usage data, identification data, communication records	Legal obligation, legitimate interests (to the extent permitted under applicable law)
Communication monitoring , including recording and reviewing calls, messages and interactions for quality assurance, training, security and regulatory compliance purposes	Communication records, call recordings, identification data, account information	Legal obligation, legitimate interests (to the extent permitted under applicable law)
Operational management and internal administration , including audits, reporting, governance, policy compliance and internal controls	Personal identification details, financial data, internal records, communication records	Legal obligation, legitimate interests
Improving products, services and customer experience , including analytics, service development, statistical analysis, training and quality assurance	Usage data, technical data, communication records, customer feedback	Legitimate interests (to the extent permitted under applicable law)
Marketing, promotions and customer engagement , including sending offers, communications and conducting market research	Personal identification details, contact details, marketing preferences, digital activity	Consent.
Managing complaints, disputes and legal claims , including investigations, enforcement of rights and legal proceedings	Personal identification details, communication records, transaction data	Legal obligation, legitimate interests
Business continuity and corporate transactions , including mergers, acquisitions, restructuring and transfer of business operations	Personal identification details, financial data, internal records	Legal obligation, legitimate interests (to the extent permitted under applicable law)
Insurance-related activities (where applicable) , including underwriting, claims handling and sharing with relevant third parties	Personal identification details, financial data, health data (where applicable), communication records	Contractual basis, legal obligation, consent (where required)

Automated processing

We may process your Personal Data using automated means where permitted by applicable law, including for fraud detection, risk assessment and service optimisation.

We will not make decisions that significantly affect you based solely on automated processing unless permitted by law and, where required, based on your explicit consent.

We may also use profiling and analysis of customer behaviour, preferences or financial position, including to assess eligibility for products or services, support risk and fraud detection, improve customer experience, and tailor products or services, where permitted by applicable law and, where required, based on your consent.

You may have the right to request further information about such processing or to request human review, where required under applicable law.

Changes to purpose

We will only use your Personal Data for the purposes for which it was collected, unless we reasonably consider that we need to use it for another purpose that is compatible with the original purpose and permitted under applicable law. Where required, we will notify you of such use.

Who do we share your Personal Data with and why?

Your Personal Data may be shared on a one-time, occasional or ongoing basis, depending on the nature of the relevant product, service or relationship. We will only share your Personal Data where permitted or required under applicable law and where necessary for legitimate business, operational or regulatory purposes.

Personal Data may be shared with recipients located within or, where permitted by applicable law, outside the Kingdom of Saudi Arabia, depending on the nature of the relevant product, service or relationship.

Why we share your Personal Data

We may share your Personal Data in the following circumstances:

1. to provide you with products and services, including through third parties
2. where you have provided your consent
3. to comply with applicable legal, regulatory or governmental requirements, including obligations relating to fraud prevention, financial crime and regulatory reporting
4. where disclosure is required to governmental, regulatory, judicial or other competent authorities, including for national security purposes or in connection with legal proceedings
5. where it is necessary for our legitimate interests, to the extent permitted under applicable law, including to manage risk, prevent fraud, protect our rights, or assess suitability for products or services, provided this does not override your rights or involve Sensitive Data

6. for operational, administrative and business continuity purposes, including internal governance and service delivery
7. in connection with corporate transactions, such as mergers, acquisitions, restructuring or transfer of business operations
8. where you have consented to receive marketing communications or to the sharing of your Personal Data for marketing purposes
9. where the Personal Data is obtained from publicly available sources in accordance with applicable law

We may also share information within or outside the ARB Group in anonymised or aggregated form, where it is no longer possible to identify you.

Where third parties process Personal Data on our behalf, we ensure that they are subject to appropriate contractual and security obligations.

We will only share the minimum amount of Personal Data necessary for the relevant purpose and only for as long as necessary to achieve that purpose.

We may share your Personal Data with the following categories of recipients:

Recipient category	Description
ARB Group entities	Our affiliates and subsidiaries within the ARB Group
Service providers and operational partners	Vendors, consultants, IT providers, cloud providers, website hosts, subcontractors, agents and other service providers who support our business operations and the delivery of our products and services
Payment and card service providers	Payment service providers, payment networks, card processors and related service providers involved in processing transactions, issuing and managing cards, and conducting fraud and risk checks
Financial institutions and market participants	Banks, lenders, financial institutions, clearing and settlement systems, brokers, asset managers and other entities involved in financial transactions or services
Credit reference and fraud prevention agencies	Credit bureaus and fraud prevention agencies that assess creditworthiness, detect fraud and verify identity
Debt collection and recovery agencies	Debt collection agencies, recovery agents and related service providers engaged to recover amounts owed to us or to manage outstanding debts.
Connected and authorised parties	Joint account holders, guarantors, beneficiaries, trustees, executors, authorised signatories, attorneys, intermediaries, correspondents or any person acting on your behalf
Third parties you approve or instruct	Social media platforms, payment providers, loyalty partners, or any third party you authorise or instruct us to share your Personal Data with
Third parties you transact with	Parties you make payments to or receive payments from, including merchants and counterparties

Recipient category	Description
Insurance-related parties	Insurers, intermediaries, underwriters, claims handlers, investigators, experts and medical professionals, where relevant to insurance products or claims
Regulatory, governmental and public authorities	Regulators, courts, law enforcement agencies, tax authorities, dispute resolution bodies and other competent authorities, including for public interest or national security purposes
Fraud, compliance and risk management bodies	Entities involved in anti-money laundering, sanctions screening, fraud detection, risk management and compliance activities
Professional advisors	External auditors, lawyers, consultants and other professional advisors, who are subject to confidentiality obligations
Dispute-related parties	Third parties involved in disputes, claims or investigations relating to you or your transactions
Transaction and corporate restructuring parties	Third parties involved in mergers, acquisitions, financing, asset sales, restructuring or potential transfers of business or assets
Other instructed or permitted recipients	Any other third party where disclosure is required by law, or where you or a person acting on your behalf instructs us to share your Personal Data

Do we use your Personal Data for marketing purposes?

We may use your Personal Data to provide you with details about our products and services or the products and services of third parties, but only where you have provided your explicit consent for us to do so.

We may also use your Personal Data to conduct market research or to identify trends relevant to our products or services, or our business generally. Third parties acting on our behalf may contact you to invite you to participate in research, but they will only use communication methods that are consistent with your communication preferences as notified to us by you.

We will not send you marketing communications unless you have provided your explicit consent.

You can change your marketing preferences or withdraw your consent to receive marketing messages at any time through the nera app, which belongs to ARB, by following this path: Settings > Notifications.

If you ask us to stop sending you marketing communications, we will seek to process your request promptly and, where possible, immediately, and in any event within 4 to 5 business days. You may continue to receive communications during this period.

The 'What are your rights?' section of this Policy contains more details on how you can change your marketing preferences and the time frame within which we will respond to your request.

Please note that, even if you ask us to stop sending you marketing communications, we may still use your contact details to send you important information, for example about changes to the products and services provided to you by us, or to comply with our regulatory or legal obligations.

If you withdraw your consent to receive marketing communications, this will not affect the lawfulness of any processing carried out before your withdrawal takes effect.

Where do we hold your Personal Data and will it be transferred outside the Kingdom?

Personal Data may be processed and stored on systems operated by Alrajhi Bank or authorised third-party service providers, including cloud-based infrastructure, which may be located within or, where permitted by applicable law, outside the Kingdom of Saudi Arabia.

By default, Personal Data is held within the Kingdom of Saudi Arabia by Alrajhi Bank, ARB Group entities, or authorised third-party service providers (as described in the “Who do we share your Personal Data with and why?” section of this Policy).

Where it is necessary to transfer your Personal Data outside the Kingdom of Saudi Arabia, we will ensure that such transfer is carried out in accordance with the PDPL and applicable regulatory requirements, including those issued by SAMA. We will also ensure that appropriate safeguards are in place to protect your Personal Data.

This may include conducting transfer risk assessments, implementing appropriate contractual safeguards, including standard contractual clauses or other transfer mechanisms recognised or approved by competent authorities, or ensuring that the recipient is subject to adequate data protection standards, in each case as required under applicable law.

If you would like further information about where your Personal Data is stored or transferred, please contact us using the details set out in the “How do you contact us?” section of this Policy.

How do we protect your Personal Data?

We are committed to protecting your Personal Data. We maintain a range of appropriate technical and organisational security measures to protect your Personal Data from unauthorised access, use, loss, disclosure or destruction. We also limit access to your Personal Data to those who have a genuine need to access it, and persons responsible for processing your Personal Data on our behalf are subject to a duty of confidentiality.

Our security measures include, but are not limited to:

1. Protection against data breaches and malicious actors/hackers;

2. Implementing relevant controls, standards, and rules as issued by the National Cybersecurity Authority to include best practices and cybersecurity standards, for example:

- Data Encryption: We make use of data encryption methods to protect data both in transit and at rest. This ensures that data remains secure even if intercepted or accessed by unauthorised parties
- Access Controls: We implement strict access controls to limit who can view or manipulate Personal Data. We also use role-based access control (RBAC) to grant permissions based on job roles and responsibilities; and
- Data Minimization: We collect and retain only the data necessary for specific purposes, and avoid gathering excessive information that may increase risk if compromised; and

3. Any requirements mandated by SAMA.

We also have procedures in place to deal with any suspected or identified data security breach. We will notify the Saudi Central Bank (SAMA) of any such breach **promptly** and in accordance with applicable regulatory requirements and, where required under applicable law, notify other competent authorities and affected individuals.

How long do we store your Personal Data?

We will not retain your Personal Data for longer than is necessary to fulfil the purposes for which it was collected, unless we are legally required or otherwise permitted under applicable law to retain it for a longer period.

This may include retention periods required under applicable banking, legal, regulatory, judicial or internal governance requirements.

Personal Data is retained in accordance with applicable laws, regulatory requirements, including those issued by SAMA, and our internal retention policies. In some cases, applicable requirements may require us to retain certain records for extended periods.

Following the end of the relevant retention period, we will securely delete, irreversibly anonymise, or otherwise ensure that the Personal Data is no longer actively processed, in accordance with applicable law.

What are your rights?

Under the PDPL, you have certain rights in relation to the processing of your Personal Data. These rights may generally be exercised free of charge, subject to applicable legal requirements.

1. **Right to be Informed**

You have the right to be informed about why your Personal Data is being collected, the legal basis for its processing, and the purposes for which it is used.

2. Right to Access and Request a copy

You have the right to access your Personal Data and request a copy of it in a clear and readable format.

3. Right to Rectification

You have the right to request that your Personal Data be corrected, completed or updated if it is inaccurate, incomplete or out of date.

4. Right to Destruction

You have the right to request erasure of your Personal Data where applicable under law. Any such request will remain subject to applicable legal, regulatory and retention requirements.

5. Right to withdraw consent

Where processing is based on your consent, you have the right to withdraw that consent at any time. Withdrawal of consent will not affect processing carried out on another lawful basis.

6. Right to complain

You have the right to lodge a complaint with the competent authority in accordance with applicable law. The Saudi Central Bank (SAMA) is the primary regulator for banking services and will typically be your first point of contact, including for matters relating to your Personal Data in the context of banking services. Where relevant, complaints relating specifically to Personal Data protection under the PDPL may also be submitted to the Saudi Data and Artificial Intelligence Authority (SDAIA) through its published channels.

7. Right to claim compensation

You have the right to seek compensation for material or moral damage if you suffer harm as a result of any violation of the PDPL or its Implementing Regulations.

If you would like to exercise any of your rights, including submitting a request to access your Personal Data (commonly referred to as a data subject access request), please contact us using the details set out in the “How do you contact us?” section below.

We may ask you for information reasonably necessary to verify your identity before processing your request.

If you would like to withdraw your consent to the processing of your Personal Data by us, you may do so by contacting us by email using the details set out in the “How do you contact us?” section below.

We will respond to requests to exercise your rights, including access requests, promptly and within the timeframes required under applicable law. In certain circumstances, this period may be extended, in which case we will inform you in advance and explain the reason for the delay. Where we are unable to comply with your request, we will explain the reasons for that decision, subject to applicable law.

You may also contact us at any time if you would like further information about your rights or how to exercise them.

How do you contact us?

If you have any questions about this Policy or the Personal Data we hold about you, or if you wish to exercise your rights under the PDPL or make a complaint, please contact our Data Protection Officer at DPD@nera.sa

How to complain

If you have any queries or concerns about how we use your Personal Data, please contact us first. We will review your concern and seek to resolve it as appropriate. You also have the right to lodge a complaint with the competent authority in accordance with applicable law. The Saudi Central Bank (SAMA) is the primary regulator for banking services and will typically be your first point of contact, including for matters relating to your Personal Data in the context of banking services.

Where relevant, complaints relating specifically to Personal Data protection under the PDPL may also be submitted to the Saudi Data and Artificial Intelligence Authority (SDAIA) through its published channels.

Nothing in this Policy prevents you from exercising any right you may have to raise concerns or complaints through other channels available under applicable law.

Changes to this Policy

Effective date: 1 September 2024

Last updated: 31 March 2026

Version: 2.0

This Policy may be updated from time to time to reflect changes in legal, regulatory or operational requirements. Any updates will be published on our website or communicated through our usual channels. This Policy is subject to periodic review and approval under Alrajhi Bank's internal governance processes to ensure that it remains accurate, up to date and compliant with applicable laws and regulatory requirements.

You should review this Policy periodically to remain informed of any updates.

This Policy should be read together with any product, service or channel-specific notices that may apply to your relationship with us

Al Rajhi Bank group companies

Company Name
Alrajhi Capital
Tahweel alrajhi
Tawtheeq
Emkan
Urpay
Neoleap
Atmaal
Ejada
Drahim
Neotek