Vision Bank Limited Privacy Policy

Introduction

Vision Bank Limited (the **"Bank"** which shall include references to **"we"** **"us"** or **"our"**) is committed to protecting your privacy in how we handle your personal data. Respecting your privacy is of paramount importance to the Bank.

This policy outlines how the Bank seeks to collect, process and store personal information about individuals ("data subjects"), hereinafter (**"you"** or **"your"**), including the Bank's customers and prospective customers.

We are subject to a set of requirements to protect the privacy, confidentiality, and security of personal information, including the *ADGM Data Protection Regulations 2021 (**"DPR"**),* as applicable, and we take those obligations seriously.

Data controller

The responsible entity for the collection, processing and use of your personal data is:

Vision Bank Limited having its registered address at:
Floor 30, Al Maqam Tower, Abu Dhabi Global Market Square
Al Maryah Island
Abu Dhabi, United Arab Emirates
P.O. Box 764603

The Bank has appointed a Data Protection Officer, who is accessible via dpo@vision-bank.com.

Data collection and processing

Data collection and processing in case of opening and using the Bank account

If you are representing our corporate customers as either a board member, staff of the senior management, shareholder, or authorized signatory, then personal data related to your identification, contact data, economic data and finance data will be processed by the Bank for the purpose of opening an account and using the services of the Bank. This includes but is not limited to the following personal data:

- Full name
- Email
- mobile
- Country of nationality
- Country of residence
- Emirates ID (if you are a UAE resident)
- Passport
- Shareholding type &ownership
- Signature specimen

Please note that it is not possible to open an account with the Bank, if you do not provide your personal data as mentioned above.

Data collection and processing when performing liveness-detection

The Bank is legally obliged to check your identity using a valid identification document while on-boarding and to store specific information from the identification document. For this purpose, we offer you a liveness-detection photo (with the combination of photo and video), via a secure transmission path. The Bank will transmit personal data to its external service providers, as data processors, for the purpose of verifying

your identity as required by law. After you authorize our banking application on your device to access your camera, you will be asked to take a photograph of yourself and record a video. In the video, you will be instructed to move and show the front and back of your personal identification document or the main page of your passport.

Please note that, since we are a digital bank with fully remote communication with our customers, we can only offer a remote check of your identity and thus need your consent to proceed therewith.

Data collection and processing when transacting using the Bank account

In order to process transactions and/or payments, the Bank receives personal data and transfers personal data according to the applicable legal and regulatory framework to payers, recipients and other financial institutions through our financial services, payments and transaction processing service providers. The personal data received by other entities in this regard concerns your account information, recipient's account information, and other transaction details like the payment reference.

Data processing when displaying in-App updates and informational communication

We use informational emails, in-App updates (in case if you use our mobile banking application) and push notifications to inform you about transactions, payments, withdrawals, and other relevant information related to your usage of our products and services. For some informational emails, in-App updates, and push notifications we analyze your user behavior (status of your account, recent transactions, withdrawals, interaction with services offered) to send you (additional) information about these processes via emails, in-App updates, or push notifications.

Data collection and processing related to relationship management

For effective relationship management and customer care, the Bank collects and utilizes personal data, including information obtained from telephonic conversations, in accordance with applicable legal and regulatory requirements. This data may include your name, contact details, details related to your accounts, your usage of our services and products, communication history, feedback from calls, and other relevant information. We use this data to provide personalized support and enhance your banking experience. Your telephonic conversations may be recorded for quality assurance, training, and dispute resolution purposes. We may share this data internally among relevant departments or with authorized third parties solely for the purpose of delivering efficient customer services and improving customer relationships.

Data collection and processing through social media plugins

On our website, we have share buttons linking to Facebook, YouTube, LinkedIn, X, and Instagram. These are not third-party plugins, and do not actively send or allow third parties to obtain personal data or any other sort of information whatsoever. The share buttons are hyperlinks that only redirect you to the respective website of the third party when clicked.

Data collection and processing related to marketing activities

Through our marketing activities, we inform you about our offers related to our financial products and services, features, referral initiatives and we may ask for your feedback or opinion via surveys. If you would like to receive marketing emails, we require an email address from you. We will only send you marketing emails if you consent.

Data collection methods

We primarily gather personal and company information when you provide it directly to us or when it is shared by a third party whose details you've given us, like your authorized representative. This information is typically collected through application forms, web forms, surveys, or via email or telephone communications (e.g., when you contact us for information or show interest in our products and services).

Additionally, we may collect your personal information through the following channels:

Public sources
Information from publicly available sources, including public registers like The Official Public Register of Abu Dhabi Global Market.

Social media
When you access our social media pages, we may collect information such as your user ID, profile picture, email address, and any information shared with us through the social media service.

Website usage
Information about your use of our website collected each time you visit, whether through internet browsing or mobile/tablet applications.

Cookies
We use cookies to enhance your website experience; however, you can manage cookie settings through your web browser preferences.

Activity records
Keeping records of your account related transactions, interactions with us, including telephone recordings, and information technology ("IT") resource usage.

Participation in activities
Your participation in activities such as surveys that may involve sharing personal information securely.

Data processing purposes
In accordance with the DPR, we are only permitted to lawfully process your personal data where,

- you have given us your consent for specific purposes which we have requested from you, including those specified below;
- the processing is necessary for the performance of a contract we have entered into with you;
- to meet our legal, regulatory and compliance obligations; and
- to protect your vital interests.

Through and for our operations, we diligently gather, hold, utilize, and share personal information to fulfill essential functions vital to our services and operations. This information acquisition is critical for various aspects, including but not limited to:

- Assessing applications for products and services, ensuring customers and prospective customers receive what they require.
- Understanding and managing customer needs effectively.
- Providing and managing customer accounts, products, and services.
- Identifying and verifying customer details, including identity, for seamless transactions.
- Confirming Know Your Customer ("KYC"), Anti Money Laundering ("AML") and World-Check statuses in compliance with legal requirements.
- Continuously developing, improving, and reviewing our offerings.
- Identifying customer behavior, habits, and preferences for enhanced service delivery.
- Conducting marketing activities to inform you about our and others' products and services.
- Maintaining accurate records, including managing consent preferences as advised by you.
- Assisting with applications, enquiries, or complaints promptly.
- Complying with legal and regulatory obligations across various laws and acts.
- Managing risks effectively to protect against fraud, misconduct, and unlawful activities.

- Managing complaints, investigations, and legal proceedings.
- Conducting research, and analysis related to our offerings.
- Facilitating asset or business transfers and related arrangements.
- Assisting regulatory authorities as needed.
- Pursuing any other lawful purpose required or permitted by law.

Security

We strive to maintain the confidentiality, integrity, and availability of your personal data and provide a secure environment for your interactions with us. To safeguard your information against unauthorized access, disclosure, alteration, or destruction, we implement robust security measures and adhere to industry best practices. These security measures include but is not limited to:

Data encryption

We use encryption technologies to secure the transmission of your data between your device and our systems. This ensures that your information remains confidential and protected during transit.

Access control

Access to your personal data is restricted to authorized personnel only. We maintain strict access controls and authentication mechanisms to prevent unauthorized access to sensitive information.

Secure storage

Your personal data is stored in secure databases and systems with restricted access. We regularly update and patch our systems to address security vulnerabilities and protect against threats.

Regular audits and monitoring

We conduct regular security audits and assessments to identify and mitigate potential risks to your data. Our systems are continuously monitored for suspicious activities and unauthorized access attempts.

Employee training

Our employees undergo comprehensive training on data protection and security practices. They are required to adhere to strict confidentiality obligations and data handling procedures.

Data minimization

We only collect and process the personal data necessary for the purposes outlined in our privacy policy. We do not retain your data longer than necessary and securely dispose of it when no longer needed.

Incident response

In the event of a data breach or security incident, we have established incident response procedures to promptly address and mitigate the impact. We will notify you and relevant authorities as required by law.

Third-party security

We ensure that third-party service providers who handle your data adhere to strict security standards and contractual obligations to protect your information.

Disclosures

We may disclose your personal data to third parties for various purposes, including data processing activities carried out on behalf of the Bank. These disclosures are governed by strict contractual agreements and comply with data protection regulations. The categories of third parties with whom we may share your data include but are not limited to:

IT Infrastructure and connection providers

We may engage third-party providers to manage our IT infrastructure and connections, ensuring the secure and efficient operation of our systems.

IT security providers
To enhance the security of your data, we work with IT security providers who implement measures to protect against cyber threats and unauthorized access.

Software and software maintenance providers
Third-party software providers assist us in delivering and maintaining software solutions that support our operations and services.

Back-office management service providers
We may utilize back-office management service providers for administrative functions and operational support.

Financial services, payments, and transaction processing providers
External providers help us to process and securely manage financial transactions, payments, and transaction-related data.

KYC providers
We may engage KYC providers to verify customer identities and comply with regulatory requirements.

Fraud prevention and identification service providers
Third-party providers assist us in detecting and preventing fraud, enhancing the security of our services.

Information/documentation automation, management & destruction providers
We work with providers to automate information management processes, securely store and manage documentation, and ensure proper data destruction when required.

Consultancy companies
External consultancy firms may be engaged for specialized services, advice, and strategic support.

In addition to the above, your data may be shared with other entities such as financial institutions, regulators, and law enforcement agencies for legal, compliance, fraud prevention, and criminal activity prevention purposes. External lawyers and consultants may also receive your data under strict confidentiality agreements to provide legal advice and consulting services.

We ensure that all third parties with whom we share your data adhere to exacting standards of data protection and confidentiality, and we take appropriate measures to safeguard your privacy rights in such disclosures.

Cross border transfers of personal data
Insofar as we transmit data to entities located outside the Abu Dhabi Global Market and in order to ensure an appropriate level of data protection equivalent to that granted under the DPR upon the international transfers of personal data, the Bank has implemented one or more of the following transfer mechanisms, if applicable:

- A decision of the ADGM Office of Data Protection deciding that the third country ensures an adequate level of protection.
- Binding Corporate Rules (“BCRs”) approved by ADGM Office of Data Protection.
- Standard data protection clauses for the transfer of personal data to third countries (“SCCs”), as adopted by ADGM Office of Data Protection.

Deletion and Retention Periods
We are storing and processing your personal data only as long as it is necessary to perform our obligations under the agreement and to satisfy any legal and regulatory obligations owed by us to you. We shall store your data with you or as long as the law requires us to store it. That means, if the data is not required

anymore for statutory or contractual obligations, your data will be deleted. This also occurs in case your on-boarding process is not finalized with the opening of an account with the Bank, and meanwhile there are still pending legal or security obligations for the Bank to preserve your data. However, that rule does not apply, if its limited processing is necessary for the following purposes:

- Performing regulatory and tax retention periods, which relate to the applicable laws and complementary regulations. The statutory retention periods and documentation obligations are six years.
- Keeping evidence in the context of statutory limitation periods. According to laws applicable to us, these limitation periods can be up to thirty years, however the regular limitation period is six years.

Furthermore, whenever your consent is the legal ground to process your personal data, the Bank will store that data for as long as you do not revoke your consent or until your account is closed, whichever happens the latest.

Privacy Rights

Right to Withdraw Consent

If you exercise your right to withdraw consent, we will cease processing your personal data for which you have withdrawn consent, unless there is another legal basis for processing that data. We will update our records to reflect your withdrawal of consent and ensure that your personal data is no longer used for the specified purposes.

Right of Access

Upon receiving a request for access to your personal data, we will promptly provide access to the requested information. We may ask for additional information to verify your identity and ensure the security of your data during this process.

Right to Data Portability

If you request data portability, we will provide your personal data in a structured, commonly used, and machine-readable format. We will facilitate the transfer of this data to another controller as per your request, ensuring compliance with data protection requirements.

Right to Erasure (Right to be Forgotten)

Upon receiving a valid request for erasure (right to be forgotten), we will delete or anonymize your personal data from our systems, provided there are no legal grounds for retaining the data. We will also inform any third parties with whom we have shared your data about the erasure request, where feasible.

Right to Restriction of Processing

If you request restriction of processing, we will limit the processing of your personal data to specific purposes or suspend processing altogether, as per your instructions. We will inform you if and when the restriction is lifted or modified.

Right to Object to Processing

Upon receiving an objection to processing, we will assess the grounds of the objection and either cease processing your data for the objected purposes or provide compelling legitimate reasons for continuing processing. We will inform you of our decision and any actions taken.

Rights in Relation to Automated Decision Making and Profiling

If automated decision making or profiling significantly affects you, you have the right to challenge the decision and request human intervention. We will review the decision, provide explanations, and involve human intervention as necessary to address your concerns.

Right to Data Accuracy and Correction

Upon receiving a request for access to or correction of your personal data, we will verify your identity and provide access to the requested information or make the necessary corrections promptly. We will update our records to ensure that your personal data is accurate, complete, and up to date.

If you wish to exercise any of your rights under this privacy policy, you may contact us at dpo@vision-bank.com.

We may require evidence of your identity as part of the process of providing you with access to your personal information or correcting your personal information.

There are no fees associated with making a request to access or correct your information. However, we may refuse to give you access to the personal information we hold about you if we reasonably believe that giving you access would pose a serious threat to the life, health, or safety of an individual, if giving access would have an unreasonable impact on the privacy of other individuals, or if the request is frivolous or vexatious. Other grounds for refusal to give access may also apply under the DPR or other applicable law.

Complaints

If you are not satisfied with how we manage your personal information in accordance with this privacy policy, you can register a complaint directly with the Bank's Data Protection Officer in the first instance.

The Bank will follow these steps to address and manage your complaint:

- make a record of your complaint.
- within 5 UAE business days of receiving a complaint, we will provide you with an explanation of our complaints process, including the relevant timeframe in which we will provide a response; and
- we will aim to investigate and resolve all complaints within 30 UAE business days of receipt of a compliant.

If you wish to make a complaint, please contact us at dpo@vision-bank.com.

If you are not satisfied with how a complaint has been handled, you can lodge a complaint directly with the ADGM Office of Data Protection. To file a complaint, kindly complete the complaint forms available here and send them via email to data.protection@adgm.com.

Marketing

Your personal Data may be used for some marketing purposes including:

- Promotional events.
- News and offers; and
- Conducting market research and surveys.

We will only send you marketing communications upon acquiring your consent. You may elect to opt-out of marketing communications by speaking to your relationship manager, by unsubscribing to our mail or exercising your privacy rights applicable under DPR.

Changes To This Policy

We may modify or replace this policy at any time. We will publish any modified or replacement policy on our website at www.vision-bank.com. Any changes come into effect upon publication.

This version of this policy applies from 26th June 2024.

How to contact us

If you have any questions, you would like to raise a concern or you would like to exercise any of the privacy rights referred to above in reference to your data, please email us on dpo@vision-bank.com.