Privacy Statement: IDBI Bank Limited, DIFC Branch

IDBI Bank Limited, DIFC Branch, Dubai ('IDBI-DIFC') is registered in the Dubai International Financial Centre (DIFC) and authorized & regulated by the Dubai Financial Services Authority (DFSA). IDBI-DIFC is currently located at Unit-09, Level-4, Currency House – Building 1, Dubai International Financial Centre (DIFC), PO Box No. 506805, Dubai, United Arab Emirates (UAE).

IDBI-DIFC and the members of the IDBI Group (the "Bank") understand how important it is to protect personal data of (but not limited to) customers, employees, third parties. Therefore, the Bank is committed to keeping any personal data provided to the Bank confidential.

This Privacy Statement is pursuant to 'DIFC Data Protection Law-2020 (DIFC Law of 5 of 2020, available at https://www.difc.ae/files/6115/9358/6486/Data_Protection_Law_DIFC_Law_No.5_of_2020.pdf)' and may be read along with this Privacy Statement. The Bank intends to notify on its Privacy Statement and accordingly this Statement is put in place. The release of this Privacy Statement confirms that the Bank agrees to protect personal data collected by the Bank from but not limited to customers, employees, third parties by complying with the extant DIFC Data Protection Law and other relevant rules and regulations of the DIFC and DFSA.

Personal Data

As per the DIFC Data Protection Law, 'Personal Data' is any information referring to an Identified or Identifiable Natural Person.

(Identifiable Natural Person means a natural living person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one (1) or more factors specific to his biological, physical, biometric, physiological, mental, genetic, economic, cultural or social identity (and "Identified Natural Person" is interpreted accordingly).

Special Categories of Personal Data (SCP)

As per the DIFC Data Protection Law, Special Categories of Personal Data (SCP) means Personal Data revealing or concerning (directly or indirectly) racial or ethnic origin, communal origin, political affiliations or opinions, religious or philosophical beliefs, criminal record, trade-union membership and health or sex life and including genetic data and biometric data where it is used for the purpose of uniquely identifying a natural person.

Collection of Personal Data/SCP

The Bank collects Personal Data/SCP in connection with providing services in the course of the normal business operations. Normally, the Bank collects the information/data of its Customers/Clients and related Individuals, vendors& service providers and related Individuals, Shareholders, Directors, Beneficial Owners, Ultimate Beneficial Owners, Authorized Signatories and Employees and of any such Individuals relevant to the business relationship (hereinafter referred as 'You').

Nature and types of Collection of data of Corporates and Individuals:

From time to time, the Bank may receive personal data via the various channels through which you communicate with us, including:

i. application forms and other relevant forms customers/you submit to us (i.e., customers'/your name, Date of Birth (DOB), place of birth, address, ID Card details/number, Passport number, place and date of issue of identification document(s), contact details, nationality, company(s) owned, annual income, occupation details, financial statements, personal assets and/or investment and/or holding loans, as well as any of personal/ corporate information which is available in the public domain.

ii. transactions made through bank account(s) with us.

iii. verification of the validity and accuracy of personal and/or relevant corporate details by any third party; etc.,

Modes and sources of collecting Personal Data/SCP

We obtain most of information directly through applications or other related forms, and from maintaining records of information provided in the course of providing services. We may also obtain information from various other sources such as credit information or identity checks, Anti-Money Laundering and Counter Financing of Terrorism databases, various watch lists declared by authorities from time to time and other publicly available sources. The information may flow through physical documents, e-mails, copies, and downloads from public websites etc.

The Bank may ask for other information voluntarily from time to time to enable it to improve its services or consider the wider needs of its customers or potential customers.

Processing Personal Data/SCP

The Bank processes the Personal Data/SCP in the capacity of a Controller. As per the DIFC Data Protection Law, 'Processing' means any operation or set of operations performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage and archiving, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, restricting (meaning the marking of stored Personal Data with the aim of limiting Processing of it in the future), erasure or destruction, but excluding operations or sets of operations performed on Personal Data by:

(a) a natural person in the course of a purely personal or household activity that has no connection to a commercial purpose; or

(b) law enforcement authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security.

Purpose of processing Personal Data/SCP

The Personal Data/SCP are normally used and processed by the Bank from time to time for meeting the Business/Compliance/Statutory and Regulatory obligations which, include, inter-alia, Anti-Money Laundering (AML)/Counter-Financing of Terrorism (CFT) obligations, Client due-diligence, internal processing for business and related client services, storage of data, legal remedial measures wherever required and for compliance of applicable laws etc.

Sharing of Personal Data/SCP

The Bank respects the privacy of its customers and is committed to keeping customers' personal data and other data confidential and secure. The bank maintains strict security standards and procedures for the purpose of protecting customers' Personal Data. The Bank may share the Personal Data to third party service providers for carrying background checks in respect of client due-diligence, wherever applicable, to support/back office services, other banks, third parties as required by law/to help the Bank in various recovery measures, fraud investigation agencies, relevant regulators, statutory authorities to comply with the statutory/regulatory/legal obligations.

IDBI entities

We transfer data across IDBI businesses and branches for various business purposes (see section 'Purpose of processing Personal Data/SCP' for the full list). We may also transfer data to centralised storage systems or to process it at a central point within IDBI for efficiency purposes. For all internal data transfers we rely on our Service Level Agreements, and on the applicable local laws and regulations.

Government, Supervisory and Judicial authorities

To comply with our regulatory obligations we may disclose data to the relevant government, supervisory and judicial authorities such as:

- Public authorities, regulators and supervisory bodies such as the central banks and other financial sector supervisors in the countries where we operate.
- Tax authorities may require us to report customer assets or other personal data such as your name and contact details and other information about your organisation. For this purpose, we may process your identification data like social security number, tax identification number or any other national identifier in accordance with applicable local law.
- Judicial/investigative authorities such as the police, public prosecutors, courts and arbitration/mediation bodies on their express and legal request.

Financial institutions

To process certain payment and withdrawal services, we may have to share information about the customer or its representative with another bank or a specialised financial company. We also share information with financial sector specialists who assist us with financial services like

- Exchanging secure financial transaction messages;
- Payments and credit transactions worldwide;
- Processing electronic transactions worldwide;
- Settling domestic and cross-border security transactions and payment transactions; or
- Other financial services organisations, including banks, superannuation funds, stockbrokers, custodians, fund managers and portfolio service providers.

Service providers and other third parties

When we use other service providers or other third parties to carry out certain activities in the normal course of business, we may have to share personal data required for a particular task. Service providers support us with activities like

- Legal, auditing or other special services provided by lawyers, notaries, trustees, company auditors or other professional advisors;

- Identifying, investigating or preventing fraud or other misconduct by specialised companies;
- Performing specialised services like postal mail by our agents, archiving of physical records, contractors and external service providers; or
- Carrying out securitisation arrangements (such as trustees, investors and the advisers).

Protection of Customers' Personal Data/SCP

When accessing the Bank's Services, customers must go through a verification and authorization process to confirm each user's identity through our KYC Process.

No data transmission over the Internet can be guaranteed as secure. If a customer's browser is appropriately configured it should tell the customer whether the information the customer is sending will be secure (generally by displaying an icon such as a padlock). The combination of a secure browser at the customer's end and the Bank's security measures provide customers with the best security currently available.

Once the Bank receives personal data, the Bank will take all reasonable steps to protect that information. If the Bank no longer needs a customer's information, the Bank will destroy or de-identify it, subject to the extant record retention guidelines.

Your Rights and Choices:

Access to and Correction of Your Personal data

You have the right to access information held about you. Your right of access can be exercised in accordance with DIFC and other applicable laws. Any access request generally comes at no cost to you, but may, where permissible, be subject to a fee to meet any extraordinary administrative costs in providing you with details of the information we hold about you.

When you contact us about a potential Personal Data error, we will endeavor to confirm or verify the information in question, then correct verified inaccuracies and respond to the original inquiry. We will endeavor to send a correction notice to businesses or others whom we know to have received the inaccurate data, where required and / or appropriate. However, some third parties and third party sites may continue to process inaccurate data about you until their databases and display of data are refreshed in accordance with their update schedules, or until you contact them personally to ensure the correction is made in their own files. The Bank will not be responsible for the same.

You may also request that we restrict, erase or otherwise process your Personal Data in line with the relevant articles providing for such rights set out in the Data Protection Law, however, subject to the Bank's requirement to restrict your rights to safeguard the public interest and the Bank's interest or in accordance with provisions in the Data Protection Law.

Liabilities of the Bank

The Bank is *not* liable for any potential loss or damages under the following conditions:

- Natural disaster, war, terrorist attack, interruption of electric power, fire, water, etc. which is beyond the Bank's control.

- Disclosure, misuse, lending/delegation to any third party, transfer of the OTP Token/security password and/or user password by you/the customer.
- Telecommunication problem(s) which are beyond the Bank's control.
- Functionality problems with customers' electronic devices.
- Cyber-attacks or malware on customer's end.
- Misuse of the Bank's services.
- Any other circumstances which are beyond the Bank's control.

Our Bank's Customers

In addition to this privacy statement, our customers must also accept and be bound by any other relevant banking policies that are issued by the Bank from time to time. Such policies may be released to our customers either by mail and/or hosting on website and/or any other electronic methods.

Contact Channel in-relation to data protection

If you want access to your personal data, correction of data ***or for information regarding our data protection policy***, you are welcome to address such inquiries to:

The Data Protection Officer IDBI Bank Limited, DIFC Branch, Dubai at the details provided herein below (**Contact Us**).

Governing Law

This notice is prepared and maintained by IDBI Bank Limited, DIFC Branch, Dubai, and is governed by the laws of DIFC. From time to time, information and/or services may be amended in accordance to upcoming changes of the governing law.

Amendments and Changes

You must agree that the Bank may amend and/or change this privacy policy and other relevant policies from time to time. All updated policies will be uploaded at e-channels or informed by mail, wherever possible.

Review of this Policy

We keep this policy under regular review. This policy was last updated in October 2020.

Contact Us

If you have any questions, comments and requests related to this Privacy Statement, or if you have any complaints related to how IDBI Bank, DIFC Branch processes your personal data, please contact the Data Protection Officer (DPO) at the following address;

IDBI Bank Limited, Unit 409, Tower-1, Al-Fattan Currency House, DIFC, Dubai, UAE. PO Box – 506805

E-mail contact: dpo@idbi.co.in, DPO Contact No: +97142244983

Date: December 28, 2020