DATA PROTECTION POLICY

EXIM BANK – Dubai
Representative office, DIFC

Contents

1. Background

1.1 The DIFC Data Protection regime

The DIFC Data Protection Law (DIFC Law No. 5 of 2020, as may be amended) (the "Law") was enacted in 2020 with effect from 1st July 2020, and repealed the earlier law, DIFC Law No. 1 of 2007 (the "Previous Law"). In addition, the DIFC has also issued the Data Protection Regulations 2020 (the "Regulations") under the Law, as well as detailed Guidance, Templates and other useful information in order to ensure compliance with the Law.

The Law is administered by the DIFC Commissioner of Data Protection (the "Commissioner"), and applies in the jurisdiction of the DIFC as follows:

- to the Processing of Personal Data by automated means;
- to the Processing of Personal Data other than by automated means where the Personal Data forms part of a Filing System or is intended to form part of a Filing System;
- to the Processing of Personal Data by a Controller or Processor incorporated in the DIFC, regardless of whether the Processing takes place in the DIFC or not;
- to a Controller or Processor, regardless of its place of incorporation, that Processes Personal Data in the DIFC[1] as part of stable arrangements, other than on an occasional basis, in the context of its Processing activity in the DIFC, including transfers of Personal Data out of the DIFC.

The Law does not apply to Processing of Personal Data by natural persons in the course of a purely personal or household activity that has no connection to a commercial purpose.

This Policy applies to the Bank in the context of its Processing activity in the DIFC through the Bank's Representative Office.

What is Personal Data?

Personal Data is any information referring to an identified or Identifiable Natural Person. In the context of Processing of Personal Data, the identified or Identifiable Natural Person to whom the relevant Personal Data relates is known as the Data Subject.

Additional protection is afforded under the Law to Special Categories of Personal Data, i.e. 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.

[1] Processing "in the DIFC" occurs when the means or personnel used to conduct the Processing activity are physically located in the DIFC, and Processing "outside the DIFC" is to be interpreted accordingly.

2. This Data Protection Policy

2.1 Responsibility for Compliance

With reference to the Law, this Data Protection Policy (the “Policy”) documents the policies and procedures relating to the Processing of Personal Data applicable to all personnel of EXIM Bank (the "Bank”, “we”, “us” or “our”) to the extent of Processing activities in the DIFC. Where capitalized terms in this Policy have specific definitions in the Law, such definitions have been detailed in Annexure 1 of this Policy.

This Policy has been designed in line with the principle of “data protection by design and by default”. The Bank ensures that it Processes Personal Data in line with principles such as data minimization at the time of determining the means for Processing and at the time of Processing itself. The Bank also ensure that, by default, only Personal Data necessary for a specified purpose is Processed and Personal Data is made accessible only to specific persons involved in the Processing of that Personal Data.

It is the responsibility of each employee of the Bank to understand their obligations under the Law and this Policy, and to ensure compliance with the Law when Processing any Personal Data in the performance of their duties. All employees must ensure that the confidentiality of Personal Data, particularly Personal Data relating to clients, is safeguarded appropriately. Any contraventions of the Law or this Policy by an employee may result in financial or other penalties imposed by the DIFC or disciplinary action against employee per HR policy.

2.2 Contact Details for Data Protection matters

Any queries relating to the Bank’s Processing activities or other matters under this Policy or the Law should be referred to Resident Representative by email (eximdubai@eximbankindia.in).

3. Data Protection Notification

In accordance with the Law, the Bank submits a Notification of Personal Data Operations (the “Notification”) on an annual basis to notify the Commissioner of its Personal Data Processing activities.

Where the Bank commences Processing Personal Data in a manner different to that described in the most recent Notification, the Bank shall submit an updated Notification to the Commissioner within fourteen (14) days of such event.

A summary of the Bank’s Notification is available on the Bank’s DIFC Public Register page.

4. Principles for legitimate and lawful Processing

In accordance with the Law, all Personal Data Processed by the Bank must be:

- Processed in accordance with a specified lawful basis under the Law (as described in Section 5 of this Policy);
- Processed lawfully, fairly and in a transparent manner in relation to a Data Subject;
- Processed for specified, explicit and legitimate purposes determined at the time of collection of Personal Data, in a way that is not incompatible with those purposes and that is relevant and limited to what is necessary in relation to those purposes;
- Processed in accordance with the application of Data Subject rights under the Law;
- accurate and, where necessary, kept up to date, including via erasure or rectification, without undue delay;
- kept in a form that permits identification of a Data Subject for no longer than is necessary for those purposes determined at the time of collection of Personal Data; and
- kept secure, including being protected against unauthorised or unlawful Processing (including transfers), and against accidental loss, destruction, or damage, using appropriate technical or organisational measures

5. Lawfulness of Processing

5.1 Lawful basis for Processing Personal Data

The Bank may only Process Personal Data where any one or more of the following lawful bases for Processing is applicable:

- a Data Subject has given consent to the Processing of relevant Personal Data for specified purposes, in accordance with the conditions for consent-based Processing under the Law;
- Processing is necessary for the performance of a contract to which a Data Subject is a party, or in order to take steps at the request of a Data Subject prior to entering into such contract;
- Processing is necessary for compliance with Applicable Law that the Bank is subject to;
- Processing is necessary in order to protect the vital interests of a Data Subject or of another natural person; and/or
- Processing is necessary for the purpose of legitimate interests pursued by the Bank or a Third Party to whom the Personal Data has been made available, subject to specific conditions in relation to legitimate interests

under the Law (*Article 13 of the Law*), except where such interests are overridden by the interests or rights of a Data Subject.

5.2 Lawful basis for Processing Special Categories of Personal Data

As a policy, we do not normally collect any Special Categories of Personal Data, unless such collection is warranted under specific circumstances.

In accordance with the Law, any Special Categories of Personal Data may only be Processed by the Bank if one or more of the following applies:

- a Data Subject has given explicit consent to the Processing of relevant Special Categories of Personal Data for specified purposes, in accordance with the conditions for consent-based Processing under the Law;

- Processing is necessary for the purpose of carrying out the obligations and exercising the specific rights of the Bank or a Data Subject in the context of the Data Subject's employment;

- Processing is necessary to protect the vital interests of a Data Subject or of another natural person, where the Data Subject is physically or legally incapable of giving consent;

- Processing relates to Personal Data that has been made public by a Data Subject;

- Processing is necessary for the establishment, exercise, or defence of legal claims (including, without limitation, arbitration, and other structured and commonly recognised alternative dispute resolution procedures, such as mediation);

- Processing is necessary for compliance with a specific requirement of Applicable Law to which the Bank is subject, in which case, the Bank must provide the relevant Data Subject with clear notice of such Processing as soon as reasonably practicable unless the obligation in question prohibits such notice being given;

- Processing is necessary to comply with Applicable Law that applies to the Bank in relation to anti-money laundering or counter-terrorist financing obligations or the prevention, detection, or prosecution of any crime;

- Processing is required for protecting members of the public against dishonesty, malpractice, incompetence or other improper conduct of persons providing banking, insurance, investment, management consultancy, information technology services, accounting or other services or commercial activities (either in person or indirectly by means of outsourcing), including any resulting financial loss;

- Processing is proportional and necessary to protect a Data Subject from potential bias or inaccurate decision making, where such risk would be

increased regardless of whether Special Category Personal Data is Processed; and/or

- Processing is necessary for Substantial Public Interest reasons that are proportionate to the aim(s) pursued, respect the principles of data protection, and provide for suitable and specific measures to safeguard the rights of the Data Subject.

6. Description of the Bank's Personal Data Processing

6.1 Categories of Personal Data Processing

The Bank will process Personal Data in relation to the following purposes:

- Information & Data Bank Administration
- Licensing & Registration
- Staff Administration

6.2 Categories of Data Subjects

Personal Data will be Processed by the Bank for the following classes of Data Subjects:

- Staff (agents and workers);
- Prospective Clients & Customers
- Service providers

6.3 Type of Personal Data

The below table details the types of Personal Data that the Bank collects from Data Subjects:

Types of Personal Data	Details
Individual details	Name, address (including proof of address), other contact details (e.g. email and telephone numbers), gender, marital status, date and place of birth, nationality, employer, job title and employment history, and family details, including their relationship
Identification details	Identification numbers issued by government bodies or agencies, such as your passport number, Emirates ID or other national identity number, tax identification number and driving licence number, including copies of such government-issued identification document

Financial information	Bank account details, income, source of wealth, net worth statements, source of funds, credit or borrowing history or other financial information
Anti-money laundering and sanctions data	Screening information received from various anti-money laundering, counter-terrorism financing and sanctions databases
Special Categories of Personal Data	Information about political affiliations or opinions or criminal record, to the extent required for compliance with Applicable Law.

As a policy, we do not normally collect any Special Categories of Personal Data, unless such collection is warranted under specific circumstances.

6.4 Lawful bases for Processing Personal Data

The table below sets out the main purposes for which the Bank Processes Personal Data as well as the corresponding lawful basis for Processing that Personal Data:

Purpose for Processing	Lawful basis for Processing
Anti-Money Laundering and other legal obligations We obtain information about our clients and their representatives and beneficial owners and others to help us comply with legislation on money laundering, terrorist financing, and sanctions. We also collect and disclose Personal Data in accordance with Applicable Law and under orders from courts and regulators. Our disclosures will be to those bodies and persons who are entitled under the Applicable Law to receive the required information. In some cases, this information may include Special Categories of Personal Data, to the extent required by us to ensure compliance with Applicable Law.	For Personal Data – **Compliance with Applicable Law that we are subject to** For Special Categories of Personal Data – **To comply with Applicable Law that applies to us in relation to anti-money laundering or counter-terrorist financing obligations or the prevention, detection, or prosecution of any crime**

Services We may obtain and/or disclose information about individuals where this is necessary or appropriate to provide services to our clients.	For Personal Data – **Performance of an engagement**
Service providers We collect information about Data Subjects in connection with their provision of services to us or their position as a representative of a provider of services to us. We do not collect Special Categories of Personal Data for this purpose, other than where we are required to do so to meet our legal obligations (see 'Anti-Money Laundering and other legal obligations' above).	For Personal Data – **Performance of an engagement**
Visitors to our office We have security measures in place at our offices, which include building access controls and may include CCTV. Images captured by CCTV are securely stored and only accessed on a need-to-know basis (e.g. to investigate an incident). Visitors to our offices may be required to sign in and sign out at building reception in accordance with the building's security policies. In addition, we may also maintain visitor records ourselves, which are securely stored and only accessible on a need-to-know basis (e.g. to investigate an incident). We do not collect Special Categories of Personal Data for this purpose.	For Personal Data – **Legitimate interests for information security and physical security purposes**
Staff Recruitment We ask Data Subjects to provide Personal Data to us as part of job applications. We will also conduct checks in order to verify identity and the information in the application as well as to obtain further information about suitability for a role within the Bank. This may include obtaining	For Personal Data – **(1) For compliance with Applicable Law that we are subject to; and (2) Legitimate interests to prevent fraud**

information from regulators, anti-money laundering databases, sanctions list, etc. In some cases, this information will include Special Categories of Personal Data, where such information is required for the purpose of pre-employment verification checks or other employment-related Processing.	
Former Staff We retain Personal Data of former staff members to the extent that we have a statutory obligation to do so.	For all Personal Data – **For compliance with Applicable Law that we are subject to**

7. Processing of Personal Data on the basis of consent

The Bank generally does not Process any Personal Data on the basis of consent since another lawful basis can usually be relied upon, as described in Section 6.4 of this Policy.

If any Processing does take place on the basis of a Data Subject's consent, the Bank will ensure that:

- consent is freely given by a clear affirmative act that shows an unambiguous indication of consent;
- consent is obtained in a manner that is clearly distinguishable, in an intelligible and easily accessible form, using clear and plain language, for each purpose for which Processing is consent-based;
- if the Bank seeks to obtain consent for matters not expressly concerned with the Processing of Personal Data, the request for consent for the Processing of Personal Data is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language;
- the Data Subject is informed of their right to withdraw consent at any time, as well as how to exercise that right, at the time consent is obtained;
- where consent has been withdrawn by the Data Subject, the Bank ceases Processing Personal Data as soon as reasonably practicable and complies with other requirements for cessation of Processing under Section 9 of this Policy;
- the ongoing validity of the consent will be assessed, taking into account the circumstances and terms of such consent;

- where consent has been assessed to be invalid based on an ongoing assessment, the Data Subject is contacted without delay and asked to reaffirm consent;

- where a Data Subject has not reaffirmed consent within a reasonable period after being contacted by the Bank, such consent shall be deemed withdrawn and applicable procedures for cessation of Processing are applied; and

- where Processing is not a Single Discrete Incident and continues on the basis of consent, the Data Subject is given the opportunity to re-affirm or withdraw consent on a periodic basis.

8. Record of Processing activities

The Bank maintains a written electronic record of the Processing activities under its responsibility which includes the following details:

- name and contact details of the Data Subjects;
- description of the Personal Data Processing being carried out;
- the purpose(s) of the Processing;
- a description of the (classes of) Data Subjects whose Personal Data is being Processed;
- a description of the class of Personal Data being Processed;
- categories of recipients to whom the Personal Data has been or will be disclosed, including recipients in Third Countries;
- identification of relevant Third Countries that Personal Data may be transferred to, including an indication as to whether such jurisdiction has been assessed as having adequate levels of protection by the Commissioner, and documentation of suitable safeguards for transfer of Personal Data to non-adequate jurisdictions (as identified by the Commissioner);
- time limits for erasure of the different categories of Personal Data, where possible; and
- general description of the technical and organisational security measures undertaken by the Bank to demonstrate its compliance with the Law, where possible.

9. Cessation of Processing of Personal Data

Where the basis for Processing changes, ceases to exist, or the Bank is required to cease Processing due to the exercise of a Data Subject's rights, the Bank shall ensure that the relevant Personal Data is:

- securely and permanently deleted;
- anonymised so that the data is no longer Personal Data and no Data Subject can be identified from the data including where the data is lost, damaged or accidentally released;
- pseudonymised; or
- securely encrypted.

Where the Bank is unable to ensure that relevant Personal Data is securely and permanently deleted, anonymised, pseudonymised or securely encrypted, such Personal Data must be archived in a manner that ensures the data is 'Put beyond further use'.

Notwithstanding any part of this Section 9, the Bank is not required to securely and permanently delete, anonymise, pseudonymise or encrypt Personal Data or put it beyond further use, where such Personal Data is necessary for the establishment or defence of legal claims or must be retained for compliance with Applicable Law. However, once such grounds no longer apply, the Bank will ensure such Personal Data is securely and permanently deleted, anonymised, pseudonymised, encrypted or Put beyond further use.

10. Transfers of Personal Data out of the DIFC

The Bank may transfer Personal Data from the DIFC to a Third Country in the following circumstances while conducting its normal business operations or providing services:

- The Bank Processes Personal Data of clients, or representatives or beneficial owners of clients, through screening databases or search engines for identity verification or background screening;
- While providing services, the Bank may require the assistance of various external professional service providers, based in or out of the DIFC;
- The Bank uses support services of various external companies to help run its business efficiently, particularly in relation to its IT systems. Some of these services (such as email hosting and data backups) may involve the service provider Processing Personal Data that has also been Processed by the Bank;
- Where the Bank uses external companies to organise or host the Bank's event, the Bank may need to provide Personal Data of event attendees to such service providers;
- The Bank may share Personal Data with its regulators or other competent authorities, where required to do so to comply with legal or regulatory requirements, or to comply with regulatory requests or court orders, as may be applicable.

The Bank transfers Personal Data to parties outside the DIFC only on a need-to-know basis or to fulfil contractual, legal, or regulatory obligations. Where transfers out of the DIFC must be made outside of these purposes, the Bank will assess such requirement on a case-by-case basis.

Where Personal Data is being transferred in a physical form by post or courier, or other physical delivery means, a delivery receipt must be obtained and kept on record.

10.1 Transfers to a jurisdiction with adequate level of protection

As part of its Processing activities, the Bank may transfer Personal Data from the DIFC to a Third Country with an adequate level of protection for that Personal Data

in that Third Country, for which the Bank is not required to obtain any additional consent from the Data Subject or make any additional notification to the Commissioner.

The Commissioner maintains a list of such jurisdictions with an adequate level of protection, which is publicly available, and may be updated by the Commissioner from time to time.

10.2 Transfers in the absence of adequate level of protection

Transfers of Personal Data to a Third Country in the absence of an adequate level of protection may take place on the condition that:

A. the Bank has provided appropriate safeguards, in the form of standard data protection clauses (as prescribed by the Commissioner) with any recipients of such Personal Data, and on condition that enforceable Data Subject rights and effective legal remedies for Data Subjects are available;

B. one of the following specific derogations applies:
   - a Data Subject has explicitly consented to a proposed transfer, after being informed of possible risks of such transfer due to the absence of an adequacy decision or appropriate safeguards;
   - the transfer is necessary for the performance of a contract between a Data Subject and the Bank or the implementation of pre-contractual measures taken in response to the Data Subject's request;
   - the transfer is necessary for the conclusion or performance of a contract that is in the interest of a Data Subject between the Bank and a Third Party;
   - the transfer is necessary for the establishment, exercise, or defence of a legal claim;
   - the transfer is necessary in order to protect the vital interests of a Data Subject or of other persons where a Data Subject is physically or legally incapable of giving consent;
   - the transfer is made in compliance with Applicable Law and data minimisation principles (as outlined in Section 2.1 and 4 of this Policy) from a register that is (i) intended to provide information to the public; and (ii) open for viewing either by the public in general or by any person who can demonstrate a legitimate interest;
   - subject to certain limitations under Article 28 of the Law, the transfer is (i) necessary for compliance with any obligation under Applicable Law to which the Bank is subject; or (ii) made at the reasonable request of a regulator, police or other government agency or competent authority;
   - subject to international financial standards, the transfer is necessary to uphold the legitimate interests of the Bank recognised in international financial markets, except where such interests are overridden by the legitimate interests of the Data Subject relating to the Data Subject's particular situation; or
   - the transfer is necessary to comply with applicable anti-money laundering or counterterrorist financing obligations that apply to the Bank or for the prevention or detection of a crime; or

C. where none of the above conditions apply, the following limited circumstances apply:
   - the transfer is not repeating or part of a repetitive course of transfers;
   - concerns only a limited number of Data Subjects;
   - is necessary for the purposes of compelling legitimate interests pursued by the Bank that are not overridden by the interests or rights of the Data Subject; and
   - the Bank has completed a documentary assessment of all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of Personal Data.

Where the Bank makes transfers any Personal Data pursuant to the limited circumstances outlined under Section 10.2 (C) above, the Bank shall inform the Commissioner accordingly and inform the relevant Data Subject of the transfer and the relevant compelling legitimate interests.

11. Safeguarding and maintaining confidentiality of Personal Data

Employees will be Processing Personal Data in the course of their duties, particularly in relation to the Bank's customers and services engagements, and are obligated to ensure any such Personal Data is Processed securely and confidentially, in compliance with the Law and this Policy. The safeguarding of Personal Data is largely a matter of common sense and care. The following principles should be followed by employees at all times:

- Personal Data should be kept confidential and should be divulged only on a need-to-know basis.

- Any discussion regarding confidential Personal Data should be conducted discretely, in a private meeting room, and not in public place.

- A "clear desk" policy should be maintained. Documents and files, whether in physical or electronic form, holding any Personal Data must be secured and only made available to authorised personnel with authorised access.

- All Personal Data held must be secured against unauthorised access and theft, in line with the Bank's security policies.

- Personal Data is only allowed to be used for the purpose for which it was originally obtained. For e.g., Personal Data obtained for the purpose of performance of an engagement cannot be used for marketing purposes, unless such additional purpose has been appropriately identified and notified in line with the Law and this Policy.

- Employees must comply with the Bank's IT Security policies at all times in order to prevent unauthorised access to the Bank's IT systems and potential Personal Data Breaches.

- All computers and laptops must be password protected and must be logged off when employees are away from their desks. Computers and laptops must be fully shut down or locked at the end of the day.

- Employees should ensure that all official electronic communications only take place through their official work accounts, such as the Bank-assigned Outlook account or Microsoft Teams account. Sharing or transferring of Personal Data over electronic means such as WhatsApp, personal email accounts, personal cloud-based drives, personal transfer devices or other personal communications applications are strictly prohibited.

- All official email communications made through an employee's Bank-assigned Outlook account must include their email signature (with the relevant data protection-related disclaimer) in the official format communicated to all employees.

- No external computer technician / consultant should be permitted to use a computer without being authorized to do so. Computer technicians should be supervised at all times.

- Physical documents containing Personal Data must be placed in cabinets, when not in use. All cabinets must be locked at the end of the day and all keys must be securely stored.

- Confidential materials including any business emails on any personal electronic devices (i.e. phones/laptops) must not be stored on, saved to or transferred to personal USB or hard disk drives, personal cloud-based servers or drives, or any other personal storage or transfer devices. This information must only be stored on the Bank's document management system, i.e. the Bank-assigned Outlook account, OneDrive account or the Bank's server. Where the use of a USB or hard drive is required for transfer of data, employees should contact Resident Representative to authorise such transfer using an official USB or hard disk drive.

- Access to documents or folders on each employee's official Outlook or OneDrive account is restricted to that employee, or to any other party to whom an access link is shared to the extent that such other party requires access to such document or folder. Employees are encouraged to regularly review access rights given to other parties to access their OneDrive documents or folders and remove such access where it is no longer required.

- Employees are bound by their employment contracts as well as the Applicable Law to maintain confidentiality of Personal Data in the context of their employment with the Bank, and may be subject to disciplinary action as per the HR policy in the case of any non-compliance or Personal Data Breaches caused by their negligence.

12. Provision of information to Data Subjects

Subject to certain exceptions under the Law (*Articles 29-30 of the Law*), the Bank is required to provide Data Subjects from whom it collects Personal Data, as well as Data Subjects whose Personal Data has been collected from another party, certain information in relation to the Bank and its Processing of such Personal Data in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

In compliance with this requirement, the Bank has made such information publicly available through its Online Privacy Policy, available at: [website link]. The Online Privacy Policy also contains further information for Data Subjects on how to contact the Bank in order to exercise their rights under the Law.

13. Rights of Data Subjects

13.1 Right to withdraw consent

Where the basis for the Processing of Personal Data is consent, the Data Subject may withdraw consent at any time by notifying the Bank using any of the methods indicated under Section 13.8 of this Policy and in the Bank's Online Privacy Policy.

Upon withdrawal of consent by a Data Subject, the Bank will immediately cease the relevant consent-based Processing as soon as reasonably practicable, in accordance with the Law and Section 9 of this Policy.

13.2 Right to access, rectification and erasure of Personal Data

A Data Subject has the right to obtain from the Bank without charge and within one (1) month of the request:

- confirmation in writing as to whether or not Personal Data relating to him is being Processed and information at least as to the purposes of the Processing, the categories of Personal Data concerned, and the recipients or categories of recipients to whom the Personal Data are disclosed;

- a copy of the Personal Data undergoing Processing in electronic form and of any available information as to its source; and

- rectification of Personal Data unless it is not technically feasible to do so, subject to specific conditions under the Law for denying such a request (*Article 33(4) of the Law*)

A Data Subject also has the right to require the Bank to erase the Data Subject's Personal Data, provided one or more of the following apply:

- the Processing of the Personal Data is no longer necessary in relation to the purposes for which it was collected;

- the Data Subject has withdrawn consent to the Processing where consent was the lawful basis for Processing and there is no other lawful basis

(following which the Bank will comply with the requirements for cessation of Processing under the Law and Section 9 of this Policy);

- the Processing is unlawful, or the Personal Data is required to be deleted to comply with Applicable Law to which the Bank is subject; or

- the Data Subject objects to the Processing and there are no overriding legitimate grounds for the Bank to continue with the Processing.

The Bank is not required to comply with a Data Subject's request for erasure of Personal Data where the Bank is required to retain that Personal Data in compliance with Applicable Law to which it is subject or for the establishment or defence of legal claims.

Where Personal Data has been rectified or erased under this Section 13.2, the Bank will communicate such rectification or erasure to each recipient to whom the Personal Data has been disclosed, unless this proves impossible or involves disproportionate effort. The Bank will also inform the Data Subject of such recipients on the Data Subject's request.

A Data Subject's exercise of their rights under this Section 13.2, and the Bank's compliance with such requests from that Data Subject, is subject to certain exceptions, restrictions, and limitations under the Law. Please refer to the Article 33 of the Law for further information.

13.3 Right to object to Processing

A Data Subject has the right to:

- object at any time on reasonable grounds relating to their particular situation to Processing of Personal Data relating to them where such Processing is carried out on the basis that it is necessary for the purposes of the legitimate interests, where applicable, of the Bank or of a Third Party;

- be informed before Personal Data is disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object to such disclosures or uses, subject to any provisions of the Law or other Applicable Law prohibiting such disclosure; and

- where Personal Data is Processed for direct marketing purposes, object at any time to such Processing.

An objection under this Section 13.3 is deemed justified unless the Bank can demonstrate compelling grounds for such Processing that overrides the interests, rights of a Data Subject.

Where such an objection is justified, the Bank will exclude such Personal Data from its Processing activities and comply with the requirements for cessation of Processing under the Law and Section 9 of this Policy.

Where Personal Data Processing has been rectified or restricted under this Section 13.3, the Bank will communicate such rectification or restriction to each recipient to whom the Personal Data has been disclosed, unless this proves impossible or involves disproportionate effort. The Bank will also inform the Data Subject of such recipients on the Data Subject's request.

13.4 Right to restriction of Processing

A Data Subject shall have the right to require a Bank to restrict Processing to the extent that any of the following circumstances apply:

- the accuracy of the Personal Data is contested by the Data Subject, for a period allowing the Bank to verify the accuracy of the Personal Data;
- the Processing is unlawful, and the Data Subject opposes the erasure of the Personal Data and requests the restriction of its use instead;
- the Bank no longer needs the Personal Data for the purposes of the Processing, but they are required by the Data Subject for the establishment, exercise, or defence of legal claims;
- the Data Subject has objected to Processing pursuant to an exercise of their rights under the Law and Section 13.3 of the Policy, pending verification of whether the legitimate grounds of the Bank override those of the Data Subject.

Where the Bank has restricted Processing of Personal Data in compliance with a Data Subject's request under this Section 13.4, and subsequently lifts the period of such restriction, it shall inform that Data Subject in writing accordingly.

In addition, where Processing of Personal Data has been restricted in accordance with this Section 13.4, the only Processing that may continue to be conducted without the consent of the Data Subject is:

- storage of the Personal Data concerned;
- Processing of the Personal Data for the establishment, exercise or defence of legal claims; and
- Processing for the protection of the rights of another person; and

Where Personal Data Processing has been restricted under this Section 13.4, the Bank will communicate such restriction to each recipient to whom the Personal Data has been disclosed, unless this proves impossible or involves disproportionate effort. The Bank will also inform the Data Subject of such recipients on the Data Subject's request.

13.5 Right to data portability

A Data Subject shall have the right to receive Personal Data that he has provided to the Bank in a structured, commonly used, and machine-readable format where the Processing is:

- based on the Data Subject's consent or the performance of a contract; and

- carried out by automated means

The Data Subject shall also have the right to have such Personal Data transmitted directly from the Bank to any other person, where technically feasible.

The Bank is not required to provide or transmit any Personal Data where doing so would infringe the rights of any other natural person.

13.6 Automated individual decision-making, including Profiling

The Bank does not Process any Personal Data through the use of Profiling or other means of automated decision-making.

13.7 Right to lodge a complaint

If a Data Subject contends that a contravention of the Law or an alleged breach of their rights has been committed by the Bank, they may lodge a complaint with the Commissioner, using the following contact details:

Address: Office of the Commissioner of Data Protection,

Dubai International Financial Centre Authority,

Level 14, The Gate, DIFC,

PO Box 74777, Dubai, UAE

Telephone: +971 4 362 2223

Website: www.difc.ae/business/operating/data-protection/

Email: commissioner@dp.difc.ae

13.8 Methods for exercising Data Subject rights

Data Subjects may contact the Bank for any queries relating to the Bank's Personal Data Processing activities or to exercise their rights under the Law by:

- sending an **email** to: eximdubai@eximbankindia.in
- sending courier at: [Export-Import Bank of India, Level 5, Tenancy 1B, Gate Precinct Building Number 3, Dubai International Financial Centre, P.O. Box: 506541, Dubai, UAE]

14. Notification of Personal Data Breaches

Where any employee becomes aware of any Personal Data Breach while carrying out their duties, the employee must promptly notify their immediate supervisor and Resident Represented by email, along with any details relating to the Personal Data Breach available with them.

Where the Bank becomes aware of, or is notified of, any Personal Data Breach, the Bank will promptly take all necessary information security and other measures to contain and mitigate the Personal Data Breach, and assess the level of risk involved and its potential impact.

The Bank will also, as soon as reasonably practicable, make Notifications to the Commissioner and/or the relevant Data Subjects of such Personal Data Breach, as may be appropriate.

14.1 Notifications to the Commissioner

If there is a Personal Data Breach that compromises a Data Subject's confidentiality, security or privacy, the Bank shall, as soon as practicable in the circumstances, notify the Personal Data Breach to the Commissioner. Such notification shall at least, either in a single notification or in phases as and when the relevant information becomes available to the Bank:

- describe the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate amount of Personal Data records concerned;

- communicate the name and contact details of the relevant person from whom more information can be obtained;

- describe the likely consequences of the Personal Data Breach; and

- describe the measures taken or proposed to be taken by the Bank to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

The Bank shall maintain a written electronic Breach Log to document any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken.

The Bank shall also fully co-operate with any investigation of the Commissioner in relation to a Personal Data Breach.

14.2 Notifications to the Data Subject

When a Personal Data Breach is likely to result in a high risk to the security or rights of a Data Subject, the Bank will communicate the Personal Data Breach to an affected Data Subject as soon as practicable in the circumstances. If there is an immediate risk of damage to the Data Subject, the Bank shall promptly communicate with the affected Data Subject. The Bank may also be required to make such communication to relevant Data Subjects where the Commissioner considers that there is a high risk to the security or rights of the Data Subjects involved.

Any such communication to the Data Subject, shall describe in clear and plain language the nature of the Personal Data Breach, shall contain at least the information provided to the Commissioner under Section 14.1 of this Policy, and

shall, where possible, make recommendations for the Data Subject to mitigate potential adverse effects.

Where communication to individual Data Subjects will involve disproportionate effort, the Bank may inform the Data Subject of such Personal Data Breach in a public communication or similar measure whereby the Data Subjects are informed in an equally effective manner.

15. Fines and sanctions for non-compliance

In accordance with Part 9 and Schedule 2 of the Law, the Commissioner may impose administrative fines, general fines and/or other penalties and sanctions to the Bank for any contraventions of the Law.

Where any such contravention is due to the action, inaction, or negligence of an employee, as may be applicable, such employee may be subject to penalties and disciplinary actions as per HR policy of the company.

DEFINED TERMS

TERM	DEFINITION
Applicable Law	Means all applicable laws, statutes, codes, ordinances, decrees, rules, regulations, municipal by-laws, judgments, orders, decisions, rulings or awards of any government, quasi-government, statutory or regulatory body, ministry, government agency or department, court, agency or association of competent jurisdiction
Controller	Means any person who alone or jointly with others determines the purposes and means of the Processing of Personal Data
Data Subject	Means the identified or Identifiable Natural Person to whom Personal Data relates
DIFC	Means the Dubai International Financial Centre
Filing System	Means any structured set of Personal Data that is accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographic basis
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)
Personal Data	Means any information referring to an identified or Identifiable Natural Person
Personal Data Breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed

Process, Processed, Processes and Processing (and other variants)	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
Processor	Means any person who Processes Personal Data on behalf of a Controller
Profiling	Means the automated Processing of Personal Data to evaluate the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the person's performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements

Put beyond further use	Means that: (a) A Controller and any relevant Processor is unable to use the Personal Data to inform any decision with respect of the Data Subject or in a manner that affects the Data Subject in any way, other than where such Personal Data needs to be cross-checked by automated means solely in order to prevent further Processing of Personal Data related to the Data Subject; (b) no party has access to the Personal Data other than the Controller and any relevant Processor; (c) Personal Data is protected by appropriate technical and organisational security measures that are equivalent to those afforded to live Personal Data; and (d) a Controller and any relevant Processor have in place and must comply with a strategy for the permanent deletion, anonymisation, pseudonymisation or secure encryption of the Personal Data, complies and can demonstrate compliance with such policy
Single Discrete Incident	Means a Processing operation or a collection of Processing operations that relate to a: (a) single, non-recurring transaction; or (b) non-recurring and clearly defined purpose that a Data Subject is seeking to achieve, in each case, with a definable end point
Special Categories of Personal Data	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
Third Country	Means a jurisdiction other than the DIFC, whether in the UAE or elsewhere
Third Party	Means any person authorized to Process Personal Data, other than the: (a) the Data Subject; (b) the Controller; or (c) the Processor

Appendix II

PRIVACY POLICY

EXIM BANK – Dubai
Representative Office, DIFC

PRIVACY POLICY

This Privacy Policy ("Policy") is designed to help you understand how we use your Personal Data, in accordance with the DIFC Data Protection Law, DIFC Law No. 5 of 2020, and the Regulations and further guidance thereunder (the "Law")[2].

We encourage you to read the whole Policy. Alternatively, if you wish to read about specific privacy practices that interest you, please click on the relevant links below.

PART A – PURPOSE

PART B – YOUR PERSONAL

PART C – OUR USE OF YOUR PERSONAL DATA

[2] https://www.difc.ae/business/operating/data-protection/

PART D – OTHER IMPORTANT

PART E – YOUR RIGHTS

PART A – PURPOSE & APPLICABILITY

1. Identity

EXIM Bank of India (Bank) is a specialized financial institution, wholly owned by Government of India. It has established a Representative Office in DIFC to conduct marketing and other liaison activities. The Representative Office does not provide any Financial or other services. Bank *inter alia* is required to comply with all legislation applicable to its activities in the DIFC.

Office Address: Exim Bank of India, Level 5, Gate Precinct Building 3, Dubai International Financial Centre, Dubai, 506541, United Arab Emirates

2. Our use of Personal Data

In connection with providing our services and in compliance with the applicable laws and regulations in the DIFC and the UAE ("Applicable Law"), we collect and Process[3] information, including Personal Data.

3. This Privacy Policy

This is our general Privacy Policy that applies to the Bank in the context of its Processing activity in the DIFC through the Bank's Representative Office.

4. Updating this Privacy Policy

This Policy may be updated from time to time. This version is dated 31st August 2020.

5. What is Personal Data?

Personal Data is any information referring to an identified or Identifiable Natural Person[4]. This includes information like your name, (e-mail) address and telephone number.

6. Our responsibility to you

We Process your Personal Data in our capacity as a Controller. This means that we are responsible for ensuring that we comply with the Law when Processing your Personal Data.

7. Contact Person for Data Protection

[3] "Processing" of Personal Data can include any one or more of the following, whether or not by automated means: 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, erasure or destruction.

[4] 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).

For any queries relating to our Data Processing activities or other matters under this Policy or the Law, you may contact us by:

- sending an email to: [eximdubai@eximbankindia.in]
- sending by post to: [Export-Import Bank of India- DIFC, Level 5, 501-B, Gate Precinct Building No 3, Dubai International Financial Centre, Dubai- 506541]

PART B – YOUR PERSONAL DATA

8. Why are we collecting Personal Data about you?

We only collect Personal Data about you in connection with providing our services and conducting our normal business operations. We may hold information about you if:

- you are a client, a representative of a client and the beneficial owner of a client.
- we are required to Process your Personal Data in accordance with Applicable Law, for e.g. anti-money laundering laws
- your information is provided to us by a client or others, or we otherwise obtain your information, in connection with the service(s) we are providing a client
- you provide services to us (or you represent a company which provides services to us)
- you represent a regulator, certification body or government body which has dealings with us
- you attend our seminars, webinars, or events, receive our newsletter updates, or visit our offices or websites
- you are an applicant for a job with us
- you are or were an employee of the Bank

9. What Personal Data do we collect about you?

The types of information we Process about you may include:

Types of Personal Data	Details
Individual details	Name, address (including proof of address), other contact details (e.g. email and telephone numbers), gender, marital status, date and place of birth, nationality, employer, job title and employment history, and family details, including their relationship to you

Identification details	Identification numbers issued by government bodies or agencies, such as your passport number, Emirates ID or other national identity number, tax identification number and driving licence number, including copies of such government-issued identification document
Financial information	Bank account details, income, source of wealth, source of funds, credit or borrowing history or other financial information
Anti-money laundering and sanctions data	Screening information received from various anti-money laundering, counter-terrorism financing and sanctions databases relating to you
Special Categories of Personal Data	Information about your political affiliations or opinions or criminal record, to the extent required for compliance with Applicable Law.

As a policy, we do not normally collect any Special Categories of Personal Data, unless such collection is warranted under specific circumstances.

Where permitted by law, we may process information about criminal convictions or offences and alleged offences for specific and limited activities and purposes, such as to perform checks to prevent and detect crime and to comply with laws relating to money laundering, fraud, terrorist financing, bribery and corruption, and international sanctions. It may involve investigating and gathering intelligence on suspected financial crimes, fraud and threats and sharing data between banks and with law enforcement and regulatory bodies.

10. Where do we collect your Personal Data from?

We may collect your Personal Data from various sources, including:

- you
- your employer
- our clients and our service providers
- anti-money laundering and counter-terrorism financing databases, sanctions list, court judgements and other databases
- government agencies and publicly accessible registers or sources of information

The sources that apply to you will depend on the purpose for which we are collecting your Personal Data. Where we obtain your information from a third party, in particular your employer or our client, we may ask them to

provide you with a copy of this Privacy Policy to ensure that you know we are Processing your information and the purpose for such Processing.

PART C – OUR USE OF YOUR PERSONAL DATA

11. How do we use your Personal Data?

In this section we set out in more detail:

- the main purposes for which we Process your Personal Data
- the lawful bases upon which we are Processing your Personal Data

Purpose for Processing	Lawful basis for Processing
Anti-Money Laundering and other legal obligations We obtain information about our clients and their representatives and beneficial owners and others to help us comply with legislation on money laundering, terrorist financing, and sanctions. We also collect and disclose Personal Data under applicable legislation and under orders from courts and regulators. Our disclosures will be to those bodies and persons who are entitled to receive the required information. In some cases, this information may include Special Categories of Personal Data, to the extent required by us to ensure compliance with Applicable Law.	For Personal Data – **Compliance with Applicable Law that we are subject to including without limitation Prevention of Money Laundering Act (PMLA), and the instructions & guidelines issued thereunder.** For Special Categories of Personal Data – **To comply with Applicable Law that applies to us in relation to anti-money laundering or counter-terrorist financing obligations or the prevention, detection, or prosecution of any crime.**
Services We may obtain information about individuals where this is necessary or appropriate to provide services to our clients.	For Personal Data – **Performance of an engagement.**
Service providers We collect information about you in connection with your provision of services to us or your position as a representative of a provider of	For Personal Data – **Performance of an engagement.**

services to us. We do not collect Special Categories of Personal Data for this purpose, other than where we are required to do so to meet our legal obligations (see 'Anti-Money Laundering and other legal obligations' above).	
Visitors to our offices We have security measures in place at our offices, which include building access controls and may include CCTV. Images captured by CCTV are securely stored and only accessed on a need to know basis (e.g. to investigate an incident). Visitors to our offices may be required to sign in and sign out at building reception in accordance with the building's security policies. In addition, we may also maintain visitor records ourselves, which are securely stored and only accessible on a need to know basis (e.g. to investigate an incident). We do not collect Special Categories of Personal Data for this purpose.	For Personal Data – **Legitimate interests for information security and physical security purposes**
Staff Recruitment We ask you to provide Personal Data to us as part of your job application. We will also conduct checks in order to verify your identity and the information in your application as well as to obtain further information about your suitability for a role within the Bank. This may include obtaining information from regulators, anti-money laundering databases, sanctions list, etc. In some cases, this information will include Special Categories of Personal Data, where such information is required for the purpose of pre-employment	For Personal Data – **(1) For compliance with Applicable Law that we are subject to; and (2) Legitimate interests to prevent fraud.** For Special Categories of Personal Data – **For carrying out our obligations and exercising our rights in the context of the Data Subject's employment.**

verification checks or other employment-related Processing.	
Former Staff We retain Personal Data of former staff members to the extent that we have a statutory obligation to do so.	For all Personal Data - **For compliance with Applicable Law that we are subject to**

12. Consent

We do not generally Process your Personal Data based on your consent (as we can usually rely on another lawful basis). Where we do Process your Personal Data based on your consent, you have the right to withdraw your consent at any time. To withdraw your consent, please contact us using the contact details mentioned in Section 7 above.

13. Do we share your information with anyone else?

We do not sell your information nor make it generally available to others. However, we may share your information in the following circumstances:

- We may Process Personal Data of clients, or representatives or beneficial owners of clients, through screening databases or search engines for identity verification or background screening.
- While providing our services, we may require the assistance of various external professional service providers, based in or out of the DIFC. The use of these external service providers may involve the service provider receiving your Personal Data from us, and some transfers of Personal Data may be made to countries or jurisdictions with data protection or privacy laws that are not adequate in comparison with the Law. Where any such transfers of Personal Data to non-adequate jurisdictions (as defined by the DIFC Commissioner of Data Protection) take place, we take appropriate data security measures to protect Personal Data in accordance with the Law.
- We use the support services of various external companies to help us run our business efficiently, particularly in relation to our IT systems. Some of these services (such as email hosting and data backups) may involve the service provider Processing your Personal Data. Some transfers of Personal Data may be made to countries or jurisdictions with data protection or privacy laws that are not adequate in comparison with the Law. Where any such transfers of Personal Data to non-adequate jurisdictions (as defined by the DIFC Commissioner of Data Protection) take place, we take appropriate data security measures to protect Personal Data in accordance with the Law.
- With other banks to help trace funds where you are a victim of suspected financial crime and you have agreed for us to do so,

or where we suspect funds have entered your account as a result of a financial crime.

- With debt collection agencies and credit reference and fraud prevention agencies.
- We may share your Personal Data with other third parties, such as relevant regulators or other authorities, where we are required to do so to comply with legal or regulatory requirements.

In each case where we share your Personal Data with other parties, whether or not in an adequate jurisdiction (as determined by the DIFC Commissioner of Data Protection), we take appropriate data security measures and ensure that the relevant party is contractually required to keep such Personal Data safe, secure and confidential in accordance with the minimum standards under the Law.

PART D – OTHER IMPORTANT INFORMATION

14. Keeping your Personal Data safe

We implement appropriate steps to help maintain the security of our information systems and processes and prevent the accidental destruction, loss, or unauthorised disclosure of the Personal Data we Process.

15. Profiling and automated decision making

We do not use profiling (where an electronic system uses Personal Data to try and predict something about you) or automated decision making (where an electronic system uses Personal Data to make a decision about you without human intervention).

16. How long do we keep your Personal Data?

We retain your Personal Data in accordance with our data retention policy which categorises all the information held by us and specifies the appropriate retention period for each category of information. Those periods are based on the requirements of the relevant laws and regulations of the DIFC and the Dubai Financial Services Authority (DFSA), and the purpose for which the information is collected and used, taking into account legal and regulatory requirements to retain the information for a minimum period, limitation periods for taking legal action, good practice and our business purposes.

17. Cross-border transfers of your Personal Data

Normally, we do not transfer Personal Data outside the DIFC, other than in the specific circumstances indicated in Section 13 above.

Where any such transfers of Personal Data to non-adequate jurisdictions (as defined by the DIFC Commissioner of Data Protection) take place, we take appropriate data security measures and put in place a contract with the

relevant third party that includes the standard international data transfer contractual terms approved by the DIFC Commissioner of Data Protection, in accordance with the Law.

PART E – YOUR RIGHTS

18. Contacting us and your rights

If you have any questions in relation to our use of your Personal Data, please email us using the contact details provided in Section 7 above.

Subject to certain exceptions outlined in the Law, you have the right to require us to:

- provide you with further details on the nature of your Personal Data held by us and the use we make of your Personal Data, including any sharing or transfer thereof;
- provide you with a copy of the Personal Data we hold about you;
- update any inaccuracies in the Personal Data we hold about you;
- delete any of your Personal Data that we no longer have a lawful basis to use or that you have withdrawn your consent for us to Process;
- where Processing is based only on consent, stop that particular Processing by withdrawing your consent;
- object to any Processing based on our legitimate interests unless our reasons for undertaking that Processing outweigh any prejudice to your data protection rights;
- restrict how we use your Personal Data during such time that the accuracy of the Personal Data, the lawful basis for Processing your Personal Data or our overriding legitimate interest in continuing to Process your Personal Data, is being contested by you; and
- transfer your Personal Data to you or a third party in a structured, commonly used and machine-readable format, to the extent that such Personal Data is automatically Processed and where the lawful basis for such Processing is your consent or for the performance of a contract.

In certain circumstances, we may need to restrict your rights in order to safeguard the public interest (e.g. the prevention or detection of crime) and our interests (e.g. responding to regulatory requests), or in accordance with other exceptions and limitations specified in the Law.

19. Your right to complain

If you are not satisfied with our use of your Personal Data or our response to any request by you to exercise your rights, or if you think that we have breached any relevant provision of the Law, then you have the right to complain to the authority that supervises our Processing of your Personal Data.

Our data protection supervisory authority is the DIFC Commissioner of Data Protection, whose contact details are as follows:

Address: Office of the Commissioner of Data Protection,
Dubai International Financial Centre Authority,
Level 14, The Gate, DIFC,
PO Box 74777, Dubai, UAE

Telephone: +971 4 362 2223
Website: www.difc.ae/business/operating/data-protection/
Email: commissioner@dp.difc.ae