BANQUE
LIBANO-FRANÇAISE

Personal Data Protection Policy

February 2021

1. Introduction

In order for Banque Libano-Française SAL (hereafter "the Bank") to cater for the needs of its different stakeholders, and especially its clients, it is bound to collect and manage personal information.

In compliance with the Lebanese law 81/2018 and the European General Data Protection Regulation (also known as the GDPR) where applicable, the Bank is committed to handling personal data in a fair, secure and transparent manner. The Bank is also committed to enabling its stakeholders to efficiently exercise their rights over their personal data.

The present policy provides an overview of the collection and processing by the Bank of personal information and outlines the data subjects' rights and their protection under the said applicable data protection laws.

This policy's scope includes, inter alia:

- Current and former clients
- Prospect clients
- Current and former shareholders and employees

It also includes any person who accesses our corporate websites:

www.eblf.com

www.luckytobeyoung.com

www.blfheadquarters.com

2. Definitions

"Personal data" means any information relating to an identified or identifiable **natural** person (hereafter "data subject").

An identifiable natural person is one 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 or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Processing" means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. Thus, processing includes: collecting, recording, organizing, structuring, storing, adapting, altering, retrieving, viewing, using, disclosing, transmitting, disseminating, making available, aligning, combining, mirroring, replicating, restricting, erasing or destroying.

"Sensitive personal data" refers to any personal data that may reveal information about a person's racial or ethnic origin, political opinion, religious beliefs, trade union activities, physical or mental health, sexual life, genetic or biometric data.

3. Data Protection Principles

The Bank is committed to the below principles:

a) Personal data will be collected and processed **lawfully**, **fairly** and in a **transparent** way.

b) Personal data will be collected only for **valid** purposes that were clearly **communicated** to data subjects and not processed in any way that is incompatible with those purposes.

c) The Bank avoids the collection and processing of **sensitive personal data**, unless required otherwise.

d) Personal data collected will be **relevant** to the purposes announced and **limited only to those purposes**.

e) Collected personal data will be **accurate** and kept **up to date**.

f) Collected personal data will be **kept only as long as necessary** for the purposes announced or as required by applicable legal/regulatory requirements.

g) Personal data will be **securely processed** with the appropriate technical and organizational measures.

4. Data Subject Rights

In the age of data, regulators all over the world are aiming to grant data subjects sufficient ownership and control over their personal data. Thus, data subjects have protected rights in regards to the collection and processing of their personal data, **subject to applicable laws and regulations**. These rights include:

- The right to access personal data.
- The right to request the correction or the updating of personal data.
- The right to request the erasure or the destruction of personal data* **.
- The right to object to or to restrict the processing of personal data*.
- The right to data portability. Data subject may request a readable copy (including, where applicable, by machine) of all the personal data they provided to the Bank.
- The right to withdraw consent at any time regarding the processing of personal data. For example, data subject may require from the Bank not to use their personal data for marketing purposes*.

**By exercising this right, the Bank may not be able to offer the data subject products and services or to pursue its relationship with them.*
*** Subject to legal and regulatory requirements which might prevent the Bank from granting such a request.*

Data subjects can exercise their rights at any time by submitting a written request. All requests relating to such rights will be dealt with promptly in accordance with applicable laws and regulations.

5. Personal Data Collection and Processing

The categories of personal data that the Bank collects and processes depend on the extent and circumstances of the relationship with the data subject and the products or services requested and/or performed.

a) Data collection through different channels

The Bank collects and processes different categories of personal data, which it receives from data subjects **in person** or via its communication channels, including its online channels.

The Bank's website uses small text files stored in a user's browser files known as cookies. Cookies are used to improve our website functionalities and also to improve the experience of its users. In order to find out information about how the Bank uses cookies please refer to the Bank's Cookie Policy.

The Bank may also collect and process personal data which it lawfully obtains from other entities within its Group[1], or other third parties (e.g. credit reference agencies, risk and compliance intelligence databases, filtering systems, public authorities).

The Bank may also collect and process personal data from publicly available sources (e.g. official governmental portals, trade registers, press, media and online databases) which it lawfully obtains and is permitted to process.

b) Types of collected and processed data

When a data subject wishes to become the Bank's client and wishes to obtain some of its products and services and when they use such products and services, personal data collected and processed may include:

- **Identification and contact data:** first name, last name, middle name, parents' names, place and date of birth, ID number, ID documents (ID card, passport, etc.), residence address, professional address, mailing address, email, telephone number, signature;
- **Tax information:** Tax Identification Number as defined by the relevant jurisdiction, tax residence, fiscal status;
- **Family status:** marital status, number of children, spouse name and occupation;
- **Employment information:** occupation, name of employer, professional income;
- **Electronic information, specifically when using online services:** identity, authentication, technical logs, connection security, IP address, etc.;
- **Financial, banking and transactional data:** assets, revenues, banking ID, card number, transaction data, loans and credits, engagements, etc.;
- **Data in relation with habits and preferences** in connection with the Bank's products and services;
- **Data related to the interactions with the Bank:** video surveillance, recorded calls, email exchange.

When the data subject wishes to benefit from the Bank's investment products and services and when using such products and services, specific information may be additionally requested, including:

- Knowledge and experience in financial instruments
- Desired investment strategy and objectives
- Components of the investment portfolio

When a data subject wishes to benefit from insurance products and services offered by the Bank's partner insurance companies and when using such products and services, requested information collected by the Bank may include specific information in regards to existing/previous policies, such as policy numbers, products,

[1] such as Banque Libano-Française SAL's representative offices, Libano-Française Finance SAL, Banque SBA SA (France), Banque SBA SA – Limassol Branch, LF Finance (Suisse) SA.

premiums, properties, claims, claims history, dependents and health data collected only following data subject's explicit consent or as permitted by regulation.

For prospective client, or non-client counterparties in a transaction with a client of the Bank, a guarantor, a security provider, a legal representative of a client or an authorized representative of a legal entity, the Bank may collect relevant personal data which may be include, inter alia, the following:

- Name, address, contact details, identification data, date and place of birth, nationality, marital status, employment status, authentication data needed by the data subject to access the Bank's digital platforms.
- For guarantors, the Bank will request personal data disclosing their economic and financial background and their credit status with other financial institutions.

The Bank understands the importance of protecting the personal data pertaining to vulnerable persons, including minors' information. No collection or processing of personal data in relation with minors occurs without first obtaining their legal guardian's consent.

6. Legal Basis for Collecting and Processing Personal Data

Understanding that personal information and the right to privacy are extremely valuable to individuals and are protected by law, the Bank does not collect or process personal information without making sure it has a proper legal basis to doing so.

a) For the performance of a contract

The Bank collects and processes personal data for the purposes of concluding and performing contracts for banking transactions with its clients and in order to offer them suitable financial services and products as well as other ancillary services. It also collects and processes such data to be able to complete its acceptance procedure of prospective clients.

b) For compliance with a legal obligation

A number of legal and regulatory obligations prescribed by relevant Lebanese and international applicable laws and regulations (commercial and banking regulations, anti-money laundering rules, financial markets regulations, tax rules, etc.) require the Bank to collect and process personal data.

This processing fulfills the Bank's obligations in terms of:

- Complying with legal obligations and regulatory requirements;
- Fighting money laundering, terrorism financing and financial crime;
- Complying with international sanctions;
- Fighting tax evasion;
- Risk management (credit risk, cyber risk, etc.).

c) For the purposes of the Bank's legitimate interests

The Bank collects and processes personal data for the purposes of fulfilling its legitimate interests. For example:

- The Bank collects and processes personal data as part of establishing legal files to be used in litigation if legal proceedings take place.
- The Bank collects and processes personal data as part of its physical and IT security systems for the prevention of potential crime, unauthorized access and for physical and asset security, admittance controls and anti-trespassing measures including the setting up of Video Surveillance systems (CCTV) for the prevention of crime or fraud.

d) Data subject consent

The Bank also collects and processes personal data as part of gathering feedback on its products and services and as part of its market research provided that prior explicit consent was obtained from the data subject by a written statement or by a clear affirmative action.

7. Personal Data Flows and Personal Data Transfer

In offering its products and services, the Bank may provide personal data to various divisions and departments within the Bank as well as to other entities within the Group.

Personal data may also be shared with service providers and suppliers enabling the Bank to perform its services. These service providers and suppliers are bound by contractual agreements with the Bank compelling them to comply with banking secrecy, confidentiality and data protection requirements.

The following recipients are examples of service providers and suppliers to whom personal data may be transferred:

- Correspondent banks, in the context of the execution of cross-border transactions;
- Brokers, counterparties and custodians in the context of transactions related to financial instruments and securities;
- Partner insurance companies in the context of gathering required data in relation to certain products and services or in the context of processing certain claims;
- Debt collection agencies and credit reference agencies;
- External legal consultants and attorneys and external auditors;
- Cards processing companies in the context of offering data subjects card services;
- Printing companies (e.g. for checkbooks printing, …);
- Airline companies and airport lounges in the context of offering loyalty programs and travel services;
- File storage, archiving and/or records management companies;
- IT companies in the context of implementing, operating, maintaining and upgrading IT systems;
- Websites and advertising agencies;

The Bank is also bound to transfer personal data to supervisory authorities and other regulatory and public authorities as per the applicable laws and regulations. For example, personal data may be transferred to:

- Banque du Liban in the context of processing certain transactions (ex. Cheques clearing)
- The Banking Control Commission (BCCL), the Special Investigation Commission (SIC) and the Capital Markets Authority (CMA), in the context of their respective supervisory role and control missions, and when answering specific requests.
- The Ministry of Finance, as required by law 55/2015 in the context of the automatic exchange of information for tax purposes (CRS).
- The United States Internal Revenue Service, as required by the Foreign Account Tax Compliance Act.
- The National Social Security Fund in the context of ensuring the Bank's employees' and their dependent family members obtain social, health and retirement benefits;
- The Income Tax unit at the Lebanese Ministry of Finance in the context of filing employees' tax returns;

Personal data may also be transferred to processors in third countries. Such processors are under the obligation to comply with the data protection principles and the Bank will only disclose personal information to third parties providing an adequate level of protection.

8. Storage and Retention of Personal Data

The Bank stores collected personal data in both physical and electronic forms. The stored data is securely retained by the Bank in accordance with the applicable laws and regulations and with the Bank's security policies and procedures.

The retention period complies with local and international applicable laws and regulations' requirements.

The retention period may be extended as required by a competent authority or if needed in the context of defending a right or a legitimate interest.

Most of the collected personal data is retained for the period covering the contractual relation and, in any case, for a period of 10 years as of the date of the relation's end.

The Bank will only retain personal data for as long as necessary to fulfill the purposes it was collected for, including those of satisfying any legal, accounting, or reporting requirements.

9. Protection measures

The Bank takes all appropriate and lawful technical, physical, legal and organizational measures against accidental or unlawful processing of data including destruction, loss, alteration, dissemination or access.

The Bank has a strict access right policy in place governing its employees' access to the its premises and IT systems. The IT Security team actively enforces the applicable security policy and monitors any breaches thereof.

In this context, the Bank reminds the data subjects to always keep their credentials private (CIF and account numbers, debit/credit card PIN, e-banking username and password, etc.) and recommends that they always make

sure to keep their cards within their sight while performing a transaction with a merchant, and to sign out of their e-banking at the end of each session. The Bank also makes sure, whenever possible, to implement two factor authentication mechanisms.

If the Bank believes that the security of its data subjects' personal data may have been compromised, it notifies them as soon as possible in accordance with applicable laws and regulations.

If data subjects have reason to believe that their personal data have been compromised, they should notify the Bank immediately.

10. Point of Contact

Should data subjects have questions or queries about their data protection policy, and wish to exercise their rights or to file a complaint, they can contact the Bank's Data Protection Officer (DPO) to this end, using this e-mail address: **data.protection@eblf.com**

11. Updates to the Bank's Data Protection Policy

This policy may need to be reviewed from time to time in order to incorporate changes that may affect the business and legal frameworks.

Any updates will be incorporated in this section of the Bank's website as soon as they occur.

The Bank strongly recommends that data subjects check the website frequently to ensure that they are advised of any updates or changes which may affect them.